OFFICECONNECT® HUB 8/TPM

3C16710

USER GUIDE

Part No.
DUA1671-0AAA03

Published
October 1997

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense: *Restricted Rights Legend:* Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for restricted Rights in Technical Data and Computer Software clause at 48 C.F.R. 52.227-7013. 3Com Technologies, c/o 3Com Centre, Boundary Way, Hemel Hempstead, Herts, HP2 7YU, UK.

For civilian agencies: *Restricted Rights Legend:* Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

CONTENTS

IMPORTANT SAFETY INFORMATION

WICHTIGE SICHERHEITSHINWEISE

L'INFORMATION DE SÉCURITÉ IMPORTANTE

YOUR HUB ADDRESSES

ABOUT THIS GUIDE

Introduction 1
How to Use This Guide 1
Conventions 2

INTRODUCTION

Networking Terminology 1-2

CREATING YOUR NETWORK

LEDs and Ports 2-1
Before You Start 2-4
Positioning the OfficeConnect Hub 2-5
Using the Rubber Feet and Stacking Clips 2-6
Wall Mounting the OfficeConnect Hub 2-7
Connecting Workstations and Other Equipment to Your Hub 2-7
Connecting OfficeConnect Hubs Together 2-8
Spot Checks 2-11

ABOUT NETWORK MANAGEMENT

3Com Network Management 3-1
Why Manage Your Hub? 3-2
Connecting to the Hub and Managing 3-3
    Managing Through the Console Port 3-4
    Managing Over the Network 3-6
Remote Management Service 3-7

Managing Your Hub Using Quick Config Manager

Installing Quick Config Manager 4-1
Installation Requirements 4-1
Installation Procedure 4-2
Running Quick Config Manager 4-2
Configuring Multiple Hubs 4-3
Quick Config Manager Window Map 4-3
Accessing the Hub 4-6
Giving the Hub an IP Address 4-7
Resetting the Hub 4-11
Initializing the Hub 4-11
Viewing the Hub 4-12
Displaying Information About the Hub 4-13
Setting Up the Alert LED 4-15
Monitoring 4-18
Monitoring Activity and Errors Statistics 4-19
Frame Types Statistics 4-21
Network Traffic Statistics 4-22
Network Errors Statistics 4-23
Configuring a Port 4-25
Hub Security 4-28
Configuring Security at Port Level 4-29
Configuring Security at Hub Level 4-31
Resilience 4-33
Setting Up a Resilient Link Pair 4-34
Using the Hub to Monitor Other Devices 4-37
Additional Management 4-39

Additional Management Using VT100

VT100 User Interface 5-1
Screens 5-1
Screen Components 5-2
Special Keystrokes 5-3
Repeater, Unit and Port Screens 5-4
Screen Map 5-4
Getting Started 5-6
Main Banner 5-6
Logon 5-7
Main Menu 5-9
Logoff 5-9
Auto Logout 5-9
Configuring and Viewing Setup Information 5-10
Setting Up Traps 5-12
Connecting a Modem to the Console Port 5-13
Configuring Local Security 5-15
Configuring Users 5-17
Creating Users 5-17
Editing Users 5-18
Deleting Users 5-19
Polling a Remote Device 5-19

Viewing Internal Version Numbers 5-20
Downloading a Software Upgrade 5-21

PROBLEM SOLVING

Isolating a Problem 6-1
Problems When Using Your Hub 6-2
Problems When Using Quick Config Manager 6-3
Problems When Using VT100 6-3
Problems When Using an IP/IPX-based Management Application 6-4

DIMENSIONS, STANDARDS AND CABLING

Dimensions and Operating Environment A-1
BABT Approval (for U.K. Users Only) A-1
Standards A-1
Cabling A-2
10BASE-T A-2
Console Port A-3

IP AND IPX ADDRESSES

IP Addresses B-1
Obtaining a Network Number B-2
How IP Addresses Work B-3
Assigning IP Addresses to a Small, Contained Network B-5
IPX Addresses B-6

TECHNICAL SUPPORT

Online Technical Services C-1
World Wide Web Site C-1
3Com Bulletin Board Service C-1
3ComFacts Automated Fax Service C-2
3ComForum on CompuServe Online Service C-3
Support from Your Network Supplier C-4
Support from 3Com C-4
Returning Products for Repair C-6

INDEX

LIMITED LIFETIME WARRANTY

EMC STATEMENTS

Important Safety Information

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all instructions carefully.*

Please read carefully the following information before installing the OfficeConnect® hub:

- Exceptional care must be taken during installation and removal of the unit.
- Only stack the OfficeConnect hub with other OfficeConnect units.
- Only use the power adapter that is supplied with the unit to ensure compliance with international safety standards.
- It is essential that the power outlet is located near the unit and is accessible. You can only remove power to the OfficeConnect hub by disconnecting the power adapter from the unit or from the socket outlet.
- This unit operates under SELV conditions (Safety Extra Low Voltage) according to IEC 950, the conditions of which are maintained only if the equipment to which it is connected is also operational under SELV.
- There are no user-replaceable fuses or user-serviceable parts inside the hub. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.
- Disconnect the power adapter before moving the unit.

WARNING: Twisted Pair RJ45 ports. *These are shielded RJ45 data sockets. They cannot be used as telephone sockets. Only connect RJ45 data connectors to these sockets.*

WICHTIGE SICHERHEITSHINWEISE

ACHTUNG: *Die Warnungen enthalten Anweisungen, die Sie zur eigenen Sicherheit zu befolgen haben.*

Lesen Sie bitte die folgenden Informationen sorgfältig durch, bevor Sie den Hub einbauen:

- Auf besondere Vorsicht muß während des Ein- und Ausbaus des Hubs geachtet werden.
- Stapeln Sie den Hub nur mit anderen OfficeConnect Hubs zusammen.
- Verwenden Sie nur das mit dem Hub mitgelieferte Netzteil um die internationalen Sicherheitsstandards zu erfüllen.
- Die Netzsteckdose muß sich in unmittelbarer Nähe des Hubs befinden und frei zugänglich sein. Sie können den Hub nur spannungsfrei schalten, indem Sie das Steckernetzteil aus der Netzsteckdose ziehen oder die Verbindung zum Gerät unterbrechen.
- Dieser Hub arbeitet mit SELV-Spannung (Safety Extra Low Voltage, Sicherheitskleinspannung) gemäß IEC950. Diese Bedingungen werden nur eingehalten, wenn die Geräte mit denen der Hub verbunden ist ebenfalls mit SELV-Spannung arbeiten.
- Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Hub haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.
- Bevor der Hub ausgebaut wird ist das Netzteil zu ziehen.

ACHTUNG: gedrehte paarfache RJ45 Anschlüsse. *Es sind abgeschirmte RJ45 Datenanschlußbuchsen. Sie dürfen nicht als Telefonanschluß verwendet werden. Verbinden Sie nur RJ45 Datenstecker mit diesen Anschlüssen.*

L'INFORMATION DE SÉCURITÉ IMPORTANTE

AVERTISSEMENT: *Les avertissements contiennent les instructions que vous devez suivre pour votre sécurité personnelle. Suivre toutes les instructions avec soin.*

Veuillez lire à fond l'information suivante avant d'installer le moyeu:

- Le soin exceptionnel doit être pris pendant l'installation et l'enlèvement du moyeu.
- Seulement entasser le moyer avec les autres moyeux OfficeConnects.
- Seulement utiliser la pièce de raccordement d'alimentation qui est fournie avec le moyeu pour assurer la conformité avec les normes de sécurité internationales.
- C'est essentiel que le socle de prise de courant du réseau soit localisé proche du moyeu et soit accessible. Vous pouvez seulement enlever l'alimentation au moyeu en débranchant la pièce de raccordement d'alimentation de l'unité ou du socle de prise de courant.
- Ce moyeu fonctionne sous les conditiones SELV (Sécurité du Voltage le plus Bas) d'après IEC950, les conditions desquelles sont maintenues seulement si le matériel à qui il est branché est aussi en exploitation sous SELV.
- Il n'y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.
- Débrancher la pièce de raccordement d'alimentation avant de remuer le moyeu.

AVERTISSEMENT: Les ports RJ45 de paire tordue. *Ceux-ci sont les socles de données RJ45 blindés. Ils ne peuvent pas être utilisés comme socles de téléphone. Seulement brancher les connecteurs de données RJ45 à ces socles.*

YOUR HUB ADDRESSES

Using Quick Config Manager, you can configure address information for your hub, which affects the way you can manage it. It is important that you note down this information as you may need to enter it when managing the hub again. Use this page to note down your settings.

If you initialize the hub, the address settings are retained to allow you to continue managing the hub. If you want to return the hub to its default address settings, you must enter them manually.

For information on configuring the hub's address settings, see "Giving the Hub an IP Address" on page 4-7.

Parameter	Default	Your Setting
Device Name	3Com	
Emergency Contact	3Com	
Support Contract	3Com	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Serial Line IP Address	192.168.101.1	
Subnet Mask	255.255.255.0	
Router IP Address	0.0.0.0	
Manager IP Address	0.0.0.0	

ABOUT THIS GUIDE

Introduction

This guide describes how to set up and manage the OfficeConnect® Hub 8/TPM. The hub is ready for use in your network. It does not require management to get it working. Management simply allows you to perform additional network functions, for example monitoring your network and adding security.

This guide is written for users who are new to networking. If you are going to manage your network for the first time, it is possible you may make mistakes. We have tried to identify the likely errors you may make and have provided hints and tips to help you recover from these situations. If you are already familiar with network management, you may be able to skip some of the information in this guide and use the information given for reference purposes.

There is a Quick Reference Guide accompanying this guide. It contains some useful information from this guide which you may need to refer to regularly.

How to Use This Guide

This table shows where to find specific information:

If you are looking for information on:	Turn to:
The hub and networking terms	Chapter 1
Creating your network	Chapter 2
What you can do with management and the different ways you can manage your hub	Chapter 3
Managing your hub using 3Com's Transcend® Quick Configuration Manager	Chapter 4
Additional management using VT100	Chapter 5
Problem solving	Chapter 6
Dimensions, standards and cabling	Appendix A
Network addressing (IP/IPX)	Appendix B
The OfficeConnect product range, obtaining technical support, and 3Com repair services	Appendix C

Conventions

The icon conventions that are used in this guide are:

Icon	Type	Description
ℹ	Information Note	Information notes call attention to important features or instructions.
⚠	Caution	Cautions alert you to personal safety risk, system damage, or loss of data.
⚡	Warning	Warnings alert you to the risk of severe personal injury.

The text conventions that are used in this guide are:

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your screen, for example: `Enter the IP address:`
Text represented as **`commands`**	**`This typeface`** is used to represent commands that you enter, for example: **`191.0.0.172`**
Keys	When specific keys are referred to in the text, they are called out by their labels, such as "the Return key" or "the Escape key," or they may be shown as [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	*Italics* are used to denote *new terms* or *emphasis*.

1 INTRODUCTION

Welcome to the world of networking with 3Com®.

In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but until now only large businesses could afford the networking advantage. The OfficeConnect® product range from 3Com changed this, bringing networks to the small office.

The OfficeConnect Hub 8/TPM is ideal for creating a small network. It is compact and attractively designed for desktop use, and is part of the OfficeConnect range which neatly stack together with clips, providing a host of facilities, for example print sharing and a network fax. For information on these products, see “3Com provides easy access to technical support information through a variety of services. This appendix describes these services.” on page C-1.

A single OfficeConnect hub allows you to create a small network with up to eight workstations, as shown in Figure 1-1.

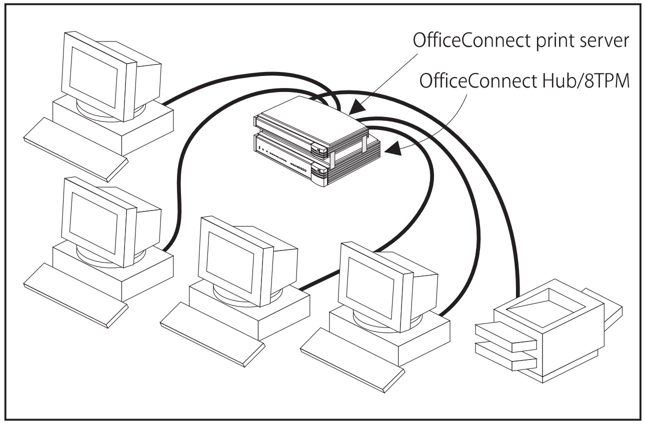


Figure 1-1 Small Network Featuring OfficeConnect Hub And Optional Print Server

If you need to connect more workstations, simply connect and clip another OfficeConnect hub to form a stack (each hub is a single repeater). The OfficeConnect Hub 8/TPM has eight 10BASE-T ports and a ninth 10BASE-2 (Coax) port. This guide helps you get the most out of your hub.

Networking Terminology

A **Network** is a collection of workstations (for example, IBM-compatible personal computers) and other equipment (for example, printers), connected for the purpose of exchanging information. Networks vary in size, some are within a single room, others span continents.

A **Local Area Network (LAN)** is a network, usually in an office, that spans no more than a single site.

Ethernet is a type of LAN, referring to the technology used to pass information around the network.

10BASE-T is the name given to the Ethernet protocol that runs over **Twisted Pair (TP)** cable. The OfficeConnect hub uses **RJ45** type connectors for connecting your network.

10BASE-2 is the name given to the Ethernet protocol that runs over **Coaxial** cable.

A **Network Loop** occurs when two pieces of network equipment are connected by more than one path. Your hub detects this and **Partitions** (isolates) one of its ports to break the loop.

A **Segment** is the length of Ethernet cable connected to a port, whether this cable is 10BASE-T, 10BASE-2 (Coax), or other type. When you daisy-chain equipment together with 10BASE-2 (Coax) cable, **all** of the cable forms a single segment.

Packets are the units of information your workstations and other equipment send to each other over the network. A **Frame** is the data part of a packet. It is the information that is seen by the hub.

Collisions are a part of normal Ethernet operation and occur if two or more devices attempt to transmit at the same time. A sudden sustained increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic. On coaxial segments an increase in collisions can also indicate faulty cabling.

Device is a term that is usually used to refer to a piece of network equipment. Every device has a unique address that is used to identify it on the network.

SNMP (Simple Network Management Protocol) is a protocol that controls how a management station gains information from a device. SNMP provides:

- A set of rules that define how a management station can communicate with a device.
- A **MIB (Management Information Base)** that defines what information can be obtained from the device by the management station. Every SNMP-manageable device has a MIB, which is a list of information about it.
- Unsolicited messages called **Traps**, which work differently to the usual request/reply management communication. You can configure a device so that it generates a trap if a certain condition occurs, for example a port partitioning. The trap is sent to the management station to inform it of the occurrence.

IP (Internet Protocol) is a data communication protocol used to connect computers and data equipment into computer networks. It is used on a large international network called the **Internet**, which is composed of universities, government facilities, research institutions and private companies. **IPX** is a Novell Netware protocol that performs a similar function to IP.

SLIP (Serial Line Internet Protocol) allows you to run the IP protocol over a serial line connection.

VT100 is a type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.

Telnet is a network application which enables a workstation to connect to a device as if it were a terminal, such as VT100. It is provided as part of IP and is commonly available with SNMP network management.

A **Modem** (Modulator-Demodulator) is a piece of equipment used for transmitting computer data over telephone lines.

2 CREATING YOUR NETWORK

All of the products in the OfficeConnect® range are designed for ease of use. This chapter describes how to use your OfficeConnect Hub 8/TPM to create your network, and has information on:

- The hub's LEDs and ports
- What you need to create your network
- Where to site the hub
- Using the rubber feet and stacking clips
- Wall mounting the hub
- Connecting your workstations and other equipment to the hub
- Connecting your hub to other OfficeConnect hubs

LEDs and Ports

The hub features diagnostic LEDs and easy to use ports.

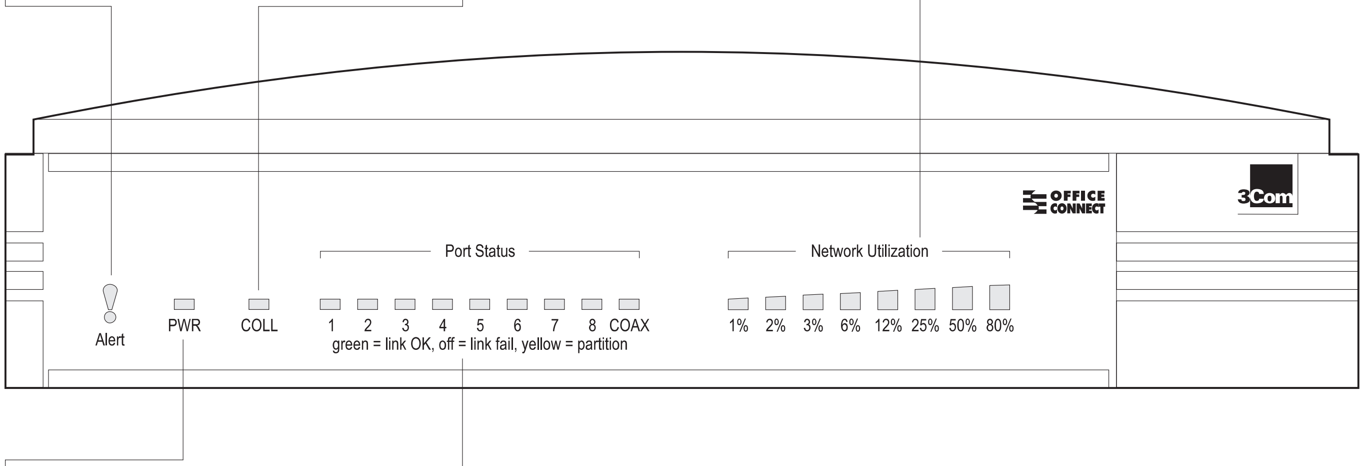
The LEDs are shown in Figure 2-1, and are used for:

- Showing you how the hub and its ports are operating
- Showing you how much your network is being used
- Alerting you to a potential problem with your network

The ports are shown in Figure 2-2, and are used for:

- Connecting workstations and other equipment to your hub
- Connecting your hub to another OfficeConnect hub
- Connecting a management station to your hub

Figure 2-1 and Figure 2-2 also appear on the Quick Reference Guide.



Alert LED
orange
Alerts you to a problem with your network. The conditions that light the LED are configurable through management, see Chapter 4.

Collision LED
yellow
Flashes each time a collision is detected on the network. Collisions are part of normal network operation.

Network Utilization LEDs
green/yellow/orange
Indicates how much your network is being used.

Power LED
green
Indicates that the power supply to the hub is present.

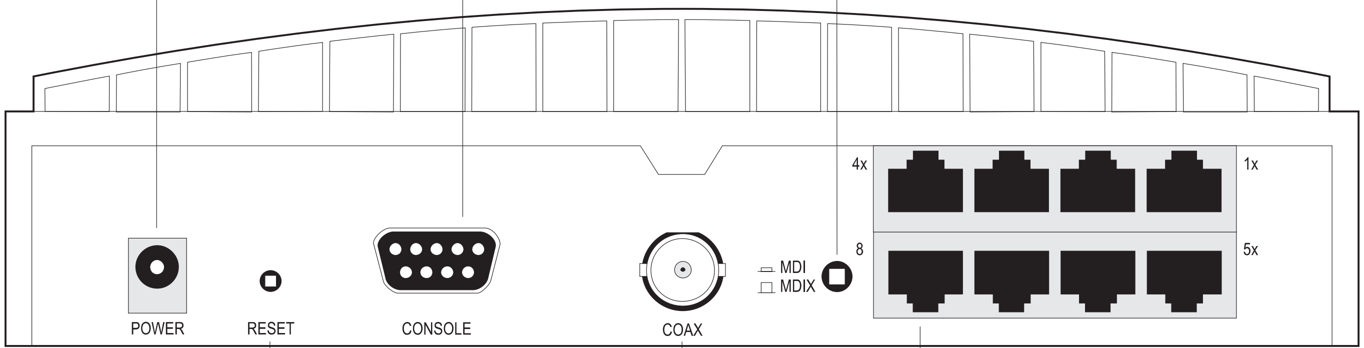
Port Status LEDs
green/yellow
Indicates the status of each port. If green, the link between the port and the next piece of network equipment is OK. If nothing is connected, the LED is off. If yellow, the port has partitioned due to a fault on that segment. The Coaxial port LED can only be yellow or off. It is yellow if the port has partitioned.

Figure 2-1 The LEDs And How To Use Them

Power Adapter socket
Only use the power adapter that is supplied with the OfficeConnect hub. Do not use any other adapter.

Console port
Can be used to connect your management station to the hub, see Chapter 3.

MDI/MDIX switch
Affects the operation of port 8. If you are connecting to a workstation, set to MDIX (out). If you are connecting to another OfficeConnect hub, set to MDI (in). See "Connecting Hubs Using 10BASE-T" on page 2-10.



Reset button
This restarts the hub, which has the same effect as powering the hub off and on.

Coaxial port
Can be used to connect your hub to other OfficeConnect hubs and equipment with 10BASE-2 cabling. If used, it is effectively a ninth port.

Eight 10BASE-T RJ45 ports
Use 10BASE-T cable with RJ45 connectors. You can connect the OfficeConnect hub to any workstation or piece of equipment that has a 10BASE-T port. Port 8 can be used to link to another OfficeConnect hub, see "Connecting Hubs Using 10BASE-T" on page 2-10.

Figure 2-2 The Ports And How To Use Them

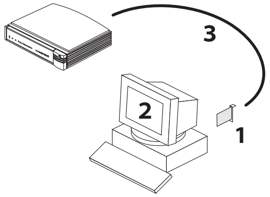
Before You Start

Your OfficeConnect hub comes with:

- One power adapter for use with the OfficeConnect hub
- A Warranty Registration card for you to fill out and return
- Four rubber feet
- Four stacking clips
- One 3.5″ Transcend® Quick Configuration Manager disk
- A Quick Reference Guide
- This guide

Workstation Connections

To connect workstations and other equipment to your hub, you need:



1 10BASE-T connections for all your equipment. 3Com produce a range of easy to install network adapters, which provide your workstations with 10BASE-T connections.

2 An operating system with network support configured, running on your workstations.

3 One ‘Straight-through’ 10BASE-T cable for every workstation or piece of equipment.
A ‘Straight-through’ cable is one where the pins of one connector are connected to the same pins of the other connector. 10BASE-T cables can be shielded or unshielded. We recommend you use shielded. The maximum length you can use is 100 meters (328 feet).

In order to comply with the 10BASE-T standard, ports designed for workstation connections have been marked with the graphical symbol 'x'. This denotes a crossover in the port's internal wiring, for example 1x, 2x, 3x...

Hub Connections

If you have additional hubs you want to connect using 10BASE-2 (Coax), you need:

- One 10BASE-2 50 Ohm cable for each additional hub. The minimum cable length you can use is 0.5 meters (1.6 feet). The maximum segment length you can have is 185 meters (607 feet).
- One 10BASE-2 'Y' piece for each hub. You can use 'T' pieces but 'Y' pieces provide adequate clearance of the other ports.
- Two 10BASE-2 50 Ohm terminators (end pieces).

If you have additional hubs you want to connect using 10BASE-T, you need:

- One 'Straight-through' 10BASE-T cable for each additional hub.

Positioning the OfficeConnect Hub

When installing your OfficeConnect hub, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines and fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. We recommend you provide a minimum of 25.4 mm (1 in) clearance.

Using the Rubber Feet and Stacking Clips

The four self-adhesive rubber feet prevent your hub from sliding around on your desk. Stick the feet to the marked areas at each corner of the underside of your hub.

The four stacking clips are used for neatly and securely stacking your OfficeConnect units together. **You can stack up to a maximum of four units. Large units must be stacked below small units.** To stack your units, secure the clips on one side and then on the other. Use the following method to secure one side:

1 Place your new unit on a flat surface. Your clips fit in the positions on the side of the unit, as shown in Figure 2-3 (1).

2 Position a clip over one of these holes and push it in until it clicks into place, as shown in Figure 2-3 (2). Repeat this for the other clip position on the same side.

3 Keeping the front of the units aligned, rest the bottom of the existing unit on the clips' spikes, as shown in Figure 2-3 (3). Push the clips firmly into the existing unit until they click into place.

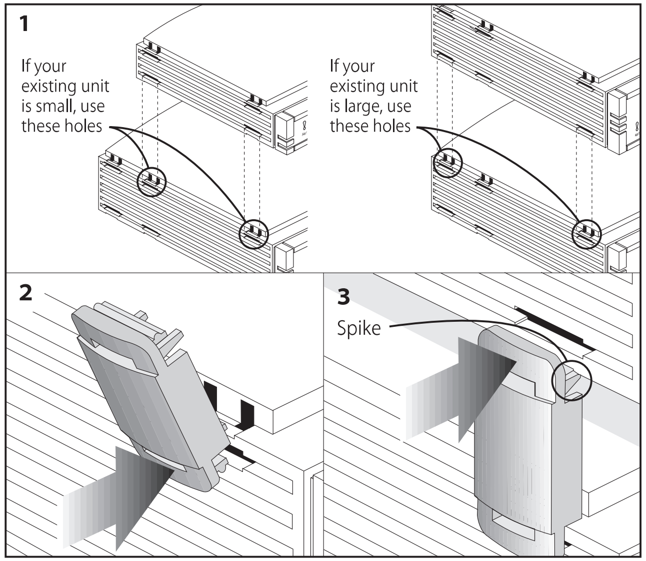

1
If your existing unit is small, use these holes
If your existing unit is large, use these holes
2
3
Spike

Figure 2-3 Clipping Your Units Together

Repeat these steps to secure the other side.

To remove a clip, hold the units firmly with one hand and hook the first finger of your other hand around the back of the clip. Use reasonable force to pull it off.

Wall Mounting the OfficeConnect Hub

There are two slots on the underside of the OfficeConnect hub which are used for wall mounting. You can mount the hub with the LEDs facing upwards or downwards, to suit your needs.

When wall mounting your hub, ensure that it is within reach of the power outlet.

You need two suitable screws. Ensure that the wall you are going to use is smooth, flat, dry and sturdy. Make two screw holes which are 142 mm (5.6 in) apart. Use the arrows at the top of the Quick Reference Guide to mark the position of the holes. Fix the screws into the wall, leaving their heads 3 mm (0.12 in) clear of the wall surface.

Remove any connections to the hub and locate it over the screw heads. When in line, gently push the hub on to the wall and move it downwards to secure. When making connections, be careful not to push the hub up and off the wall.

CAUTION: *Only wall mount single hubs, do not wall mount stacked hubs.*

Connecting Workstations and Other Equipment to Your Hub

WARNING: *Ensure you have read the Important Safety Information section carefully before you start.*

ACHTUNG: *Versichern Sie sich, daß Sie den Abschnitt mit den wichtigen Sicherheitshinweisen gelesen haben, bevor Sie das Gerät benutzen.*

AVERTISSEMENT: *Assurer que vous avez lu soigneusement la section de L'information de Sécurité Importante avant que vous commenciez.*

CAUTION: *Do not power the hub off and on quickly. Wait about 5 seconds between power cycles.*

Connecting workstations and other equipment to your hub is easy. Connect them using 10BASE-T cables to any of the hub's eight 10BASE-T RJ45 ports.

10BASE-T cables are very easy to use. To connect a 10BASE-T cable, simply slot the connector into the relevant RJ45 port. When the connector is fully in, its latch locks it in place. To disconnect the cable, push the connector's latch in and remove it.

The hub detects all port connections, so you can start using your network immediately. When you need more ports, simply add more OfficeConnect hubs.

If you are using port 8 to connect a workstation, ensure the MDI/MDIX switch is set to MDIX.

If you do not use the 10BASE-2 (Coax) port, you do not need to terminate it with a terminator (end piece).

Connecting OfficeConnect Hubs Together

You can increase the number of workstations that can connect to your network by adding more OfficeConnect hubs. You can use either 10BASE-T or 10BASE-2 (Coax) to do this:

- With 10BASE-2 (Coax) you can connect up to 30 hubs on a single segment, leaving all of the RJ45 ports free.
- With 10BASE-T you can connect up to four hubs in series.

CAUTION: *Do not connect the same two hubs together using both 10BASE-T and 10BASE-2 (Coax). This causes a network loop.*

Connecting Hubs Using 10BASE-2 (Coax)

When using 10BASE-2 (Coax) cable, it is important that both ends of the segment are properly terminated with 50 Ohm terminators (end pieces).

Only use 50 Ohm 10BASE-2 (Coax) cables and use a 'Y' piece for each hub. You can use 'T' pieces but 'Y' pieces provide adequate clearance of the other ports.

Connect a 10BASE-2 'Y' piece to each of your hubs. Daisy-chain each 'Y' piece with 10BASE-2 (Coax) cable to form a single segment, as shown in Figure 2-4. Remember to terminate the two free ends of the segment by fitting terminators (end pieces).

To disconnect a 10BASE-2 (Coax) cable, twist each connector counter-clockwise to unlock it, and remove it.

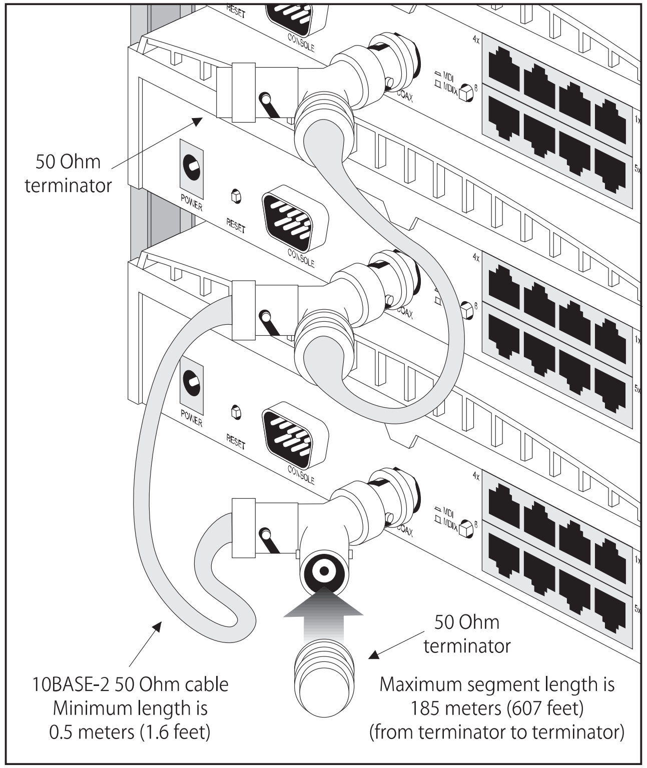

50 Ohm terminator
POWER
RESET
CONSOLE
COAX
MDI
MDI-X
50 Ohm terminator
10BASE-2 50 Ohm cable Minimum length is 0.5 meters (1.6 feet)
Maximum segment length is 185 meters (607 feet) (from terminator to terminator)

Figure 2-4 Correct Hub Connections Using 10BASE-2 (Coax)

Connecting Hubs Using 10BASE-T

You can connect hubs together with 10BASE-T in a number of ways, but for simplicity we recommend the following method:

1 Starting from the bottom, connect port 8 of the lower hub to port 7 of the hub immediately above. Repeat for each hub, as shown in Figure 2-5.

2 Set all MDI/MDIX switches to MDI (in) except for the top hub (the one with port 8 not connected to another hub). This unused port can be connected to a workstation provided that the MDI/MDIX switch is set to MDIX (out).

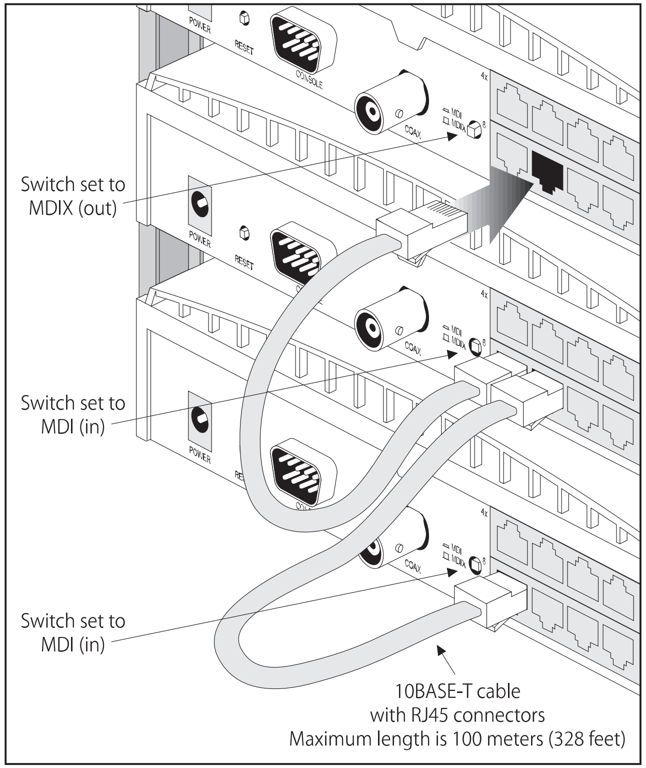


Figure 2-5 Correct Hub Connections Using 10BASE-T

Checking Hub Connections

When you have connected your hubs, power them on. The Port Status LEDs for the ports you have used should be green for 10BASE-T, or off for 10BASE-2 (Coax). If they are not, check your connections.

If the 10BASE-2 (Coax) port is not used and is not terminated, the LED should be yellow showing that it has partitioned. This is correct operation.

Spot Checks

At frequent intervals, visually check that:

- The Alert LED is not lit — this is the best way to find out if there are problems with your network
- Case vents are not obstructed
- Cabling is secure and not pulled taut

If you suspect there is a problem, refer to Chapter 6.

3 About Network Management

Network management is not required to get your hub working, it simply allows you to change the way it works and to monitor what is happening to your network. Each OfficeConnect® Hub 8/TPM is a separate manageable entity, that means you manage each OfficeConnect Hub 8/TPM individually. This chapter lists the management tasks you can perform, and describes the ways you can connect your management station to your hub. This guide uses **'Management Station'** to refer to the piece of equipment you are using to manage the hub.

Transcend Quick Configuration Manager, referred to as **'Quick Config Manager'** in this guide, is supplied with your hub and provides an easy-to-use graphical management system, through the hub's console port. Quick Config Manager uses a familiar Windows® interface with point and click operation. To use it effectively, you need to be familiar with Microsoft Windows. For information on Microsoft Windows, refer to the Microsoft Windows User's Guide.

You can also manage your hub using a VT100 terminal or any Telnet facility that emulates a VT100 terminal. VT100 uses a text-based user interface.

3Com Network Management

Quick Config Manager provides a subset of the functionality that is present in other 3Com management applications, for example the IP/IPX-based Transcend® Enterprise Manager for Windows (version 4.x and above).

Whether your network is large or small, its ongoing performance, growth and security are only as good as its management system.

Using intelligent 3Com software distributed throughout the network, 3Com's Transcend management applications support all of today's platforms and manage a wide variety of 3Com products. This gives you total control over your entire 3Com network from a single management station.

For further information about which Transcend management application can benefit your growing network, call your local sales office, see "3Com provides easy access to technical support information through a variety of services. This appendix describes these services." on page C-1.

Why Manage Your Hub?

With management, you can change and view the way your hub and network operates:

- Configure IP information for the hub so that an IP-based network management station can communicate with it.
- Restart the hub to refresh its statistics and use any new configurations.
- Initialize the hub to return it to its factory settings (IP and console port information is retained).
- Display a graphical representation of the hub to quickly view the status of each port.
- Display general hub information.
- Configure the Alert LED to light for a number of conditions, and show what conditions have triggered the Alert LED to come on.
- Graphically display network information for each port and the hub.
- Enable and disable ports.

- Configure security for the hub, including setting up new users and specifying what equipment is allowed to communicate through the hub.
- Set up resilience; specify a backup connection that takes over should a main connection fail.
- Configure the hub to send messages over the network or a modem link, to an IP/IPX-based management application (for example, Transcend Enterprise Manager), reporting the state of the hub and the network.
- Use the hub to monitor other devices on your network and report any deviation from their normal operation to an IP/IPX-based management application.
- Poll a remote device to see if it is operational.
- View any faults that have occurred with the hub.
- Download any future software upgrades to the hub.

Connecting to the Hub and Managing

Managing your hub is easy. There are many ways you can connect your management station to your hub, as shown in Figure 3-1.

You can manage the hub:

- Through the console port
  - Using Quick Config Manager
  - Using a VT100 Terminal Emulator
  - Using a VT100 Terminal
- Over the network
  - Using an IP/IPX-based Network Manager
  - Using a VT100 Terminal Emulator through Telnet

For information on using modems as part of your management connection, see "Remote Management Service" on page 3-7.

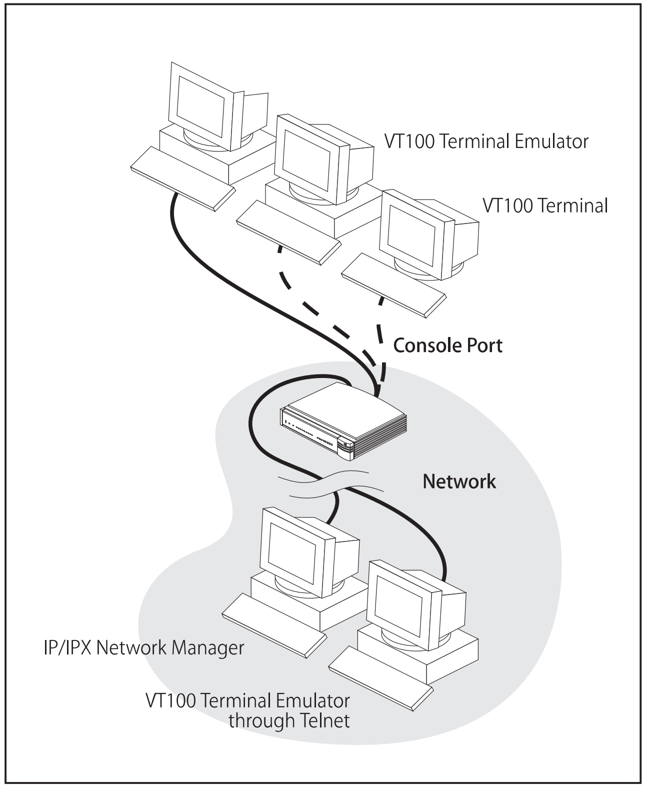


Figure 3-1 Different Management Connections To The Hub

Managing Through the Console Port

This section describes how to connect and set up equipment to communicate with the hub through the console port (called *out-of-band* management).

By default, the hub automatically configures its baud rate. The maximum rate the autoconfiguration function detects is 19200 baud.

You need to use a null modem cable for connection to the hub's console port. This is available from your supplier. The null modem cable must:

- Have a 9 pin female 'D' connector for connection to your hub, and the appropriate connector for connection to your management station.
- Not exceed 15 meters (50 feet).

There are a variety of null modem cables that you can use. For an example of one of these, see "Cabling" on page A-2.

Connection to the console port may be direct or through modems, giving the option of local or remote management. For information on managing through modems, see "Remote Management Service" on page 3-7.

Using Quick Config Manager

Connect one end of the null modem cable to the console port on the hub, and the other to the serial (RS232) port on your management station.

Quick Config Manager uses SLIP to manage your hub. When you have made your connection and installed Quick Config Manager, you are ready to manage your hub.

Refer to Chapter 4 for information on installing and using Quick Config Manager.

Using a VT100 Terminal Emulator

Connect one end of the null modem cable to the console port on the hub, and the other to the serial (RS232) port on your management station. You need to set the character size (8), stop bit (1) and parity (none) settings of your management station to work with the hub.

Press [Return][Return] to start the communication.

The management station you are using needs to run suitable terminal emulation software. Many VT100 terminal emulation packages are available.

Microsoft Windows has a terminal emulation program called 'HyperTerminal' (for Windows 95) or 'Terminal' (for other Windows versions).

Refer to the documentation that accompanies your particular terminal emulation package for details, or consult your supplier if you need further advice.

Refer to Chapter 5 for information on performing additional management using the VT100 management interface.

Using a VT100 Terminal

Connect one end of the null modem cable to the console port on the hub, and the other to the serial (RS232) port on your VT100 terminal. You need to set the character size (8), stop bit (1) and parity (none) settings of your VT100 terminal to work with the hub.

Press [Return][Return] to start the communication.

Refer to Chapter 5 for information on performing additional management using the VT100 management interface.

Managing Over the Network

This section describes how to set up equipment to allow you to communicate with the hub over the network (called *in-band* management).

Before you can manage your hub over the network using IP, you must connect to its console port locally and use Quick Config Manager to enter IP information for the hub:

1. Connect one end of a null modem cable to the console port on the hub, and the other to the serial (RS232) port on your management station.
2. Install Quick Config Manager and use it to configure the necessary IP information for the hub.

Refer to Chapter 4 for information on installing and using Quick Config Manager.

If using IPX, you do not need to enter IPX information for the hub.

Using an IP/IPX-based Network Management Application

3Com's Transcend network management applications enable you to get the best out of your hub. Any IP/IPX-based network management application can manage the hub.

The use of IP/IPX-based network management applications is not described in this manual. Refer to the user documentation that accompanies your application, for more information.

Using a VT100 Terminal Emulator (over Telnet)

Any VT100 terminal emulator that uses Telnet should be able to communicate with the hub over the network. Up to three active management sessions can access the hub concurrently. If a connection to a session is not closed, but is lost inadvertently, the connection is closed by the hub after between 2 and 3 minutes of inactivity.

Refer to the documentation that accompanies your particular terminal emulation package for details, or consult your supplier if you need further advice.

Refer to Chapter 5 for information on performing additional management using the VT100 management interface.

Remote Management Service

The OfficeConnect hub has a special modem dial-out feature which can be set up by your supplier to inform them when your hub or network is operating incorrectly. This allows your supplier to know immediately when certain problems occur, so they can act on it, leaving you to carry on with your work.

Contact your supplier to find out if they are offering a support service based on this feature.

4 MANAGING YOUR HUB USING QUICK CONFIG MANAGER

This chapter describes how to install and use Quick Config Manager. For an overview of what you can do when managing the hub, see Chapter 3.

The sections in this chapter are in the order you would normally perform them when managing the hub for the first time. If you are new to network management, read through this chapter to learn about the different management you can perform.

Quick Config Manager has a comprehensive help system that has the same useful information as this chapter.

ℹ *Before you can manage with Quick Config Manager, you must make a connection to the hub's console port, see Chapter 3.*

ℹ *In the descriptions of the options given in this chapter, the default values are underlined.*

Installing Quick Config Manager

Installation Requirements

Quick Config Manager requires an IBM compatible PC with at least a 486/33 processor. Your system must also include:

- Microsoft Windows® 3.1
  or Windows for Workgroups 3.11
  or Windows 95.
- MS-DOS 5.0 or later (not needed for Windows ‘95).
- Minimum of 4MB available hard disk space.
- Minimum of 8MB RAM. All RAM above the first megabyte must be configured as extended memory.
- 3.5″ disk drive.
- VGA or SVGA color monitor.
- Mouse.
- Serial port capable of 9600 baud, no Parity, 8bit Data, 1 StopBit.

Installation Procedure

Quick Config Manager can be installed on its own or on to a workstation that already has other Transcend® management applications installed on it.

CAUTION: *Do not install Quick Config Manager in the same directory as any other Transcend management applications. The default directory into which Quick Config Manager is installed is C:\QUICKMGR. This can be changed during the installation if required.*

The installation program is a standard Windows based installation. To install Quick Config Manager:

1 Start Windows.

If you already have an existing Transcend management application running, ensure that it is closed down.

2 Insert the Quick Config Manager disk into your disk drive.

3 In the Program Manager window, select the *Run* command from the *File* menu.

4 In the *Command Line* box, type ***`drive`*****`:\SETUP`** (where ***`drive`*** is the letter of your 3.5" disk drive) and click on OK.

The installation program starts and checks your system configuration; enter any information that's requested. The installation program reports when it has completed the installation.

When the Quick Config Manager installation is complete, it has its own program group called Transcend. If other Transcend management applications are present, the existing Transcend program group now includes Quick Config Manager.

Running Quick Config Manager

Whenever you want to start the Quick Config Manager application, double-click on the Quick Configuration Manager icon.

CAUTION: *Do not run Quick Config Manager in parallel with any other Transcend management application.*

Before you can manage your hub, you must make a connection to the hub, see Chapter 3.

If you are going to manage over a serial link from your management station, Quick Config Manager uses COM1 as the default serial port. You can change this by editing the following line under the [slip] subsection of the QUICKMGR.INI file:

```
SerialAttrib=COM1:9600,n,8,1
```

Editing it to **`SerialAttrib=COM2:9600,n,8,1`** changes the default serial port to COM2.

Configuring Multiple Hubs

There is a special feature which allows you to connect your management station to a new OfficeConnect® Hub 8/TPM without needing to close and reopen Quick Config Manager. This is particularly useful if you have many OfficeConnect hubs that need configuring or monitoring.

This feature only works if all the hubs you are going to connect to have the same baud rate (or are set to Auto Config) as the management station.

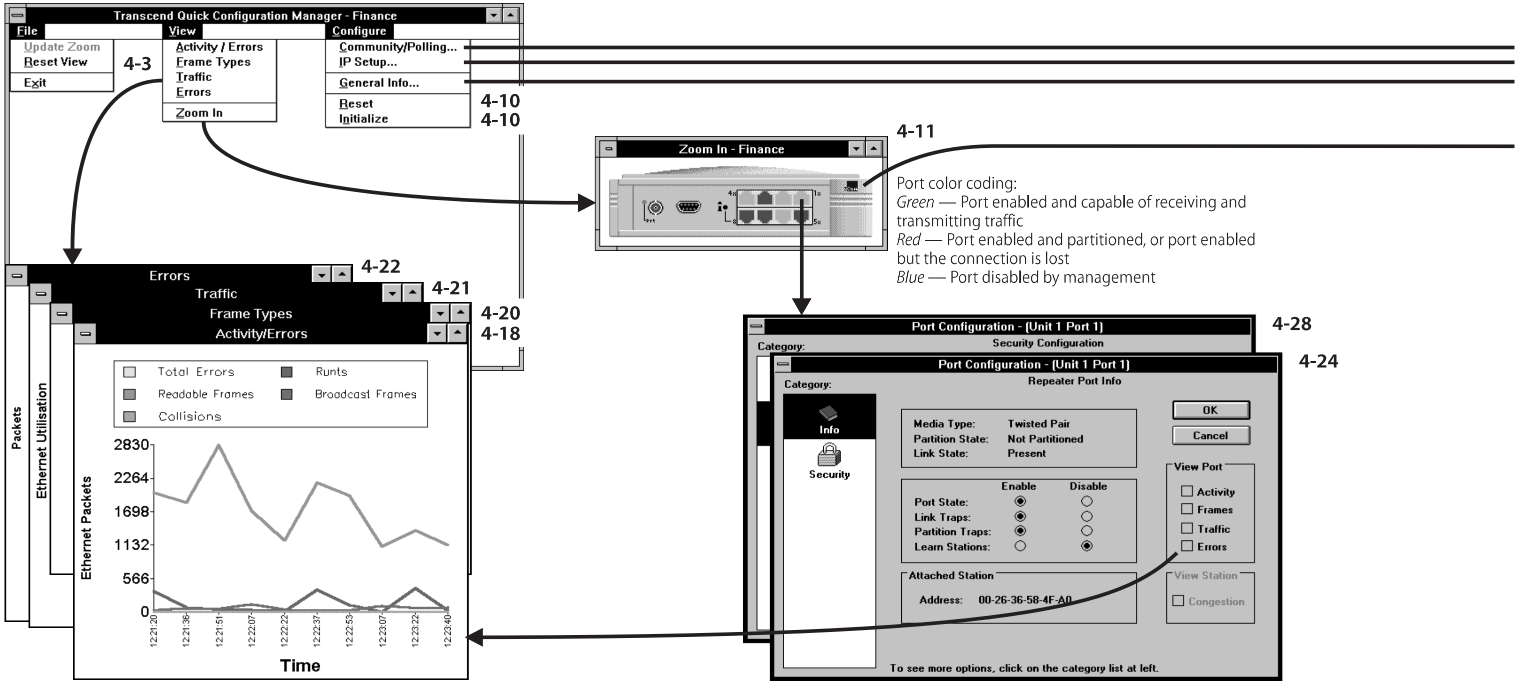
To do this:

1. Make your serial connection to the new hub.
2. From the *File* menu, select *Reset View*.

   Quick Config Manager closes any windows that are open in preparation for the new management session.

Quick Config Manager Window Map

Figure 4-1 (over the page) shows how all of the Quick Config Manager windows are accessed. This diagram also appears on the Quick Reference Guide. The number at the top right-hand side of each window refers to the page that describes the window.



Port color coding:
Green — Port enabled and capable of receiving and transmitting traffic
Red — Port enabled and partitioned, or port enabled but the connection is lost
Blue — Port disabled by management

Port Configuration - [Unit 1 Port 1]

Category: Security Configuration

Port Configuration - [Unit 1 Port 1]

Category: Repeater Port Info

Info

Security

Media Type: Twisted Pair
Partition State: Not Partitioned
Link State: Present

	Enable	Disable
Port State:	●	○
Link Traps:	●	○
Partition Traps:	●	○
Learn Stations:	○	●

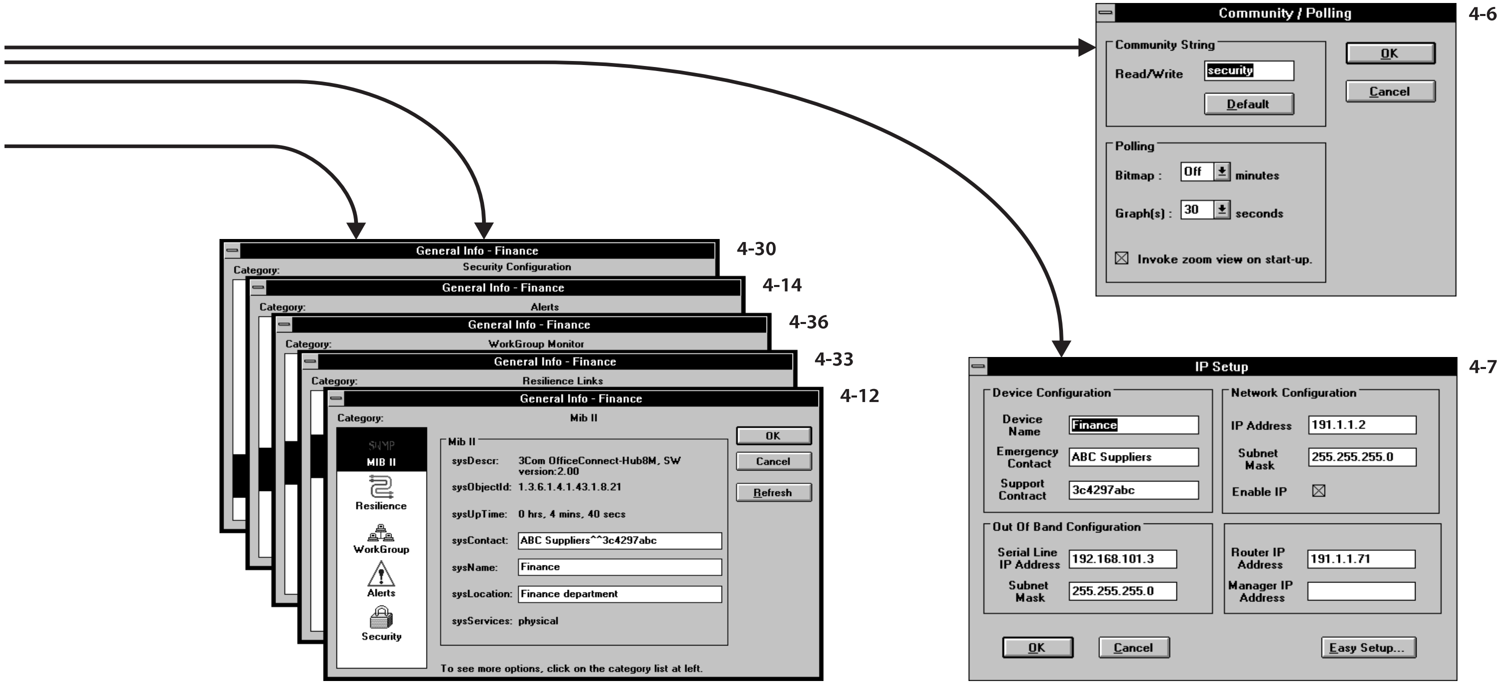
View Port
□ Activity
□ Frames
□ Traffic
□ Errors

Attached Station
Address: 00-26-36-58-4F-A0

View Station
□ Congestion

To see more options, click on the category list at left.

Figure 4-1 Quick Config Manager Window Map



Community / Polling

Community String

Read/Write: security

Default

OK

Cancel

Polling

Bitmap : Off minutes

Graph(s) : 30 seconds

☒ Invoke zoom view on start-up.

IP Setup

Device Configuration

Device Name: Finance

Emergency Contact: ABC Suppliers

Support Contract: 3c4297abc

Network Configuration

IP Address: 191.1.1.2

Subnet Mask: 255.255.255.0

Enable IP ☒

Out Of Band Configuration

Serial Line IP Address: 192.168.101.3

Subnet Mask: 255.255.255.0

Router IP Address: 191.1.1.71

Manager IP Address:

OK Cancel Easy Setup...

General Info - Finance (Category: Security Configuration)

General Info - Finance (Category: Alerts)

General Info - Finance (Category: WorkGroup Monitor)

General Info - Finance (Category: Resilience Links)

General Info - Finance

Category: Mib II

SNMP MIB II
Resilience
WorkGroup
Alerts
Security

Mib II

sysDescr: 3Com OfficeConnect-Hub8M, SW version:2.00

sysObjectId: 1.3.6.1.4.1.43.1.8.21

sysUpTime: 0 hrs, 4 mins, 40 secs

sysContact: ABC Suppliers^^3c4297abc

sysName: Finance

sysLocation: Finance department

sysServices: physical

OK Cancel Refresh

To see more options, click on the category list at left.

Accessing the Hub

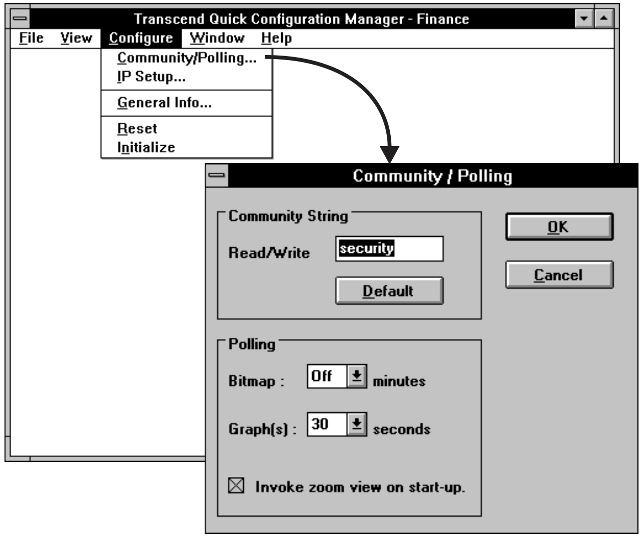
The OfficeConnect Hub 8/TPM uses *community strings* as a security measure, to check management access to the hub. The community string you use must match one of the community strings configured for the hub. Quick Config Manager remembers the last community string used. The default community strings are:

- *security* — allows you to view and configure the hub's information
- *public* — allows you to view the hub's information

To enter the community string:

1. Double-click on the Quick Config Manager icon to start the application.
2. From the *Configure* menu, select *Community/Polling.*

   Quick Config Manager displays the Community/Polling dialog box, as shown in Figure 4-2.
3. Enter the community string in the box.
4. Click on *OK*.



Community String

Read/Write: security

Polling

Bitmap : Off minutes

Graph(s) : 30 seconds

☒ Invoke zoom view on start-up.

Figure 4-2 Community/Polling Dialog Box

Changes made to this dialog box will only take effect for new windows. Any graphs or zoom view windows that are already open will continue to use the old values. Close these windows and reopen them to use the new values.

You can also use the Community/Polling screen to:

- Automatically display a graphical representation of the hub every time you start Quick Config Manager.
- Define how regularly the graphical representation of the hub is updated.
- Define how regularly any displayed graphs are updated.

Bitmap Off / 15 / 30 / 45 / 60
The time in minutes between consecutive updates of the graphical representation of the hub. If Off is selected, the bitmap is not updated at all (you can select *Update Zoom* from the *File* menu to display any new states).

Graph(s) 15 / 30 / 45 / 60
The time in seconds between consecutive updates of any graphs that are displayed.

Invoke zoom view on start-up Check this box if you want the graphical representation of the hub to be displayed every time you start Quick Config Manager.

Through VT100 management you can configure new users for the hub (with different community strings), see "Configuring Users" on page 5-17.

Giving the Hub an IP Address

You can configure the hub with an IP address and other useful information, enabling it to communicate over (become part of) an IP network.

The hub does not need an IP address to make your Quick Config Manager work with it.

You need to give your hub an IP address if you want to use an IP-based network manager, for example Transcend Enterprise Manager, to manage it over the network.

CAUTION: *If you have no previous knowledge of IP, see "IP Addresses" on page B-1.*

The IP Setup dialog box is used to set up IP information and change the SLIP address for the hub.

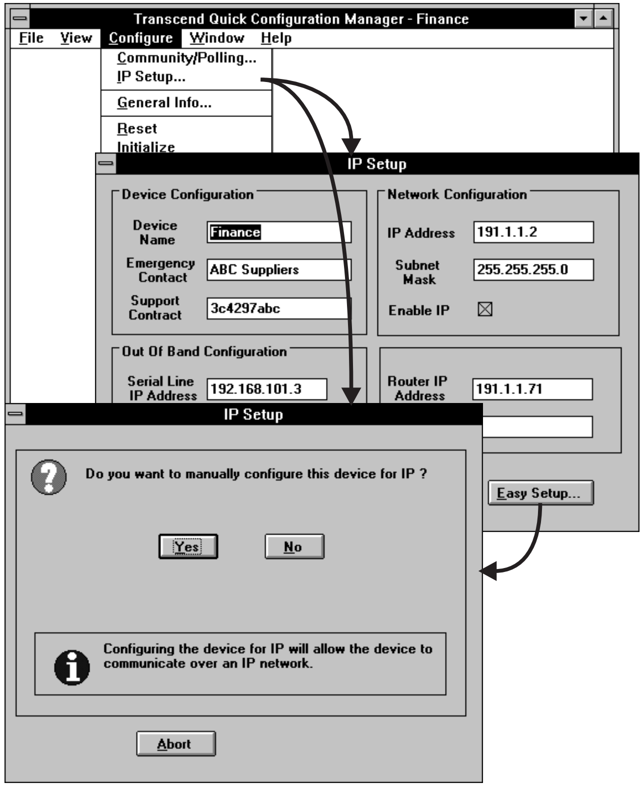
The IP Setup dialog box has a useful Easy Setup option which takes you through the IP configuration process. The information that you enter during the Easy Setup process is the same as, and is entered into, the IP Setup dialog box.

To display the IP Setup dialog box and view or configure the hub's address settings:

1 From the *Configure* menu, select *IP Setup...*

Quick Config Manager displays either the IP Setup dialog box or the Easy Setup Option, as shown in Figure 4-3, depending on what IP information is currently configured for the hub:

- If an IP address has been configured for the hub, and it is not 0.0.0.0, the IP Setup dialog box is displayed. If you have previously configured address information for the hub but want to go through the Easy Set-Up option again, you can start it by clicking on the *Easy Set-Up* button.
- If no previous IP information has been configured for the hub or the IP address is configured as 0.0.0.0, and the Enable IP box is checked, the Easy Setup option is started. If you want to enter information directly into the IP Setup screen or abort the Easy Setup process, select *Abort*.
  The Easy Setup option asks you if you want to manually configure the hub for IP. If you have a BOOTP server (that automatically allocates IP addresses) select *No*, otherwise select *Yes*.



Device Name: Finance
Emergency Contact: ABC Suppliers
Support Contract: 3c4297abc
IP Address: 191.1.1.2
Subnet Mask: 255.255.255.0
Enable IP: ☒
Serial Line IP Address: 192.168.101.3
Router IP Address: 191.1.1.71

Do you want to manually configure this device for IP ?

Configuring the device for IP will allow the device to communicate over an IP network.

Figure 4-3 IP Setup Dialog Box And Easy Setup Option

2 Enter the relevant information into the IP Setup diolog box or Easy Setup screens and click on *OK* to exit the screens.

3 Reset the hub for any changes to take effect, see "Resetting the Hub" on page 4-11.

After resetting the hub, you may need to select *Reset View* from the *File* menu to restart communication using the new information.

CAUTION: *Always make a note of any changes you make to the settings on this screen. There is an area at the front of this User Guide for doing this, called "Your Hub Addresses".*

Device Configuration Shows the following:

- *Device Name* — Provides a box for you to type a name for the hub. Use a descriptive name, for example 'Finance'.
- *Emergency Contact* — Provides a box for you to type the name and/or telephone number of your network administrator (possibly yourself) who should be contacted in an emergency.
- *Support Contract* — Provides a box for you to type the ID number of any technical support contract you may have.

The default entries for these three fields is '3Com'. These defaults are just place holders and should be changed for your information as soon as possible.

These three fields use the same information as sysContact and sysName in the MIB II panel, so if you change them, the fields in the MIB II panel change as well. For information on the MIB II panel, see "Displaying Information About the Hub" on page 4-13.

Network Configuration Shows the following:

- *IP Address* — Provides a box for you to type the IP address of the hub.

CAUTION: *To ensure that Quick Config Manager can always communicate with the hub, the IP subnet 192.168.101.x is permanently assigned to the SLIP port in addition to the user configurable SLIP address. Do not use this subnet for your Ethernet (network).*

- *Subnet Mask* — Provides a box for you to type the subnet mask for the IP address.
- *Enable IP* — If disabled, the IP fields for this dialog box are blanked and grayed-out. If enabled, the IP fields are enabled, allowing you to enter your IP information. If you are not going to manage the hub over the network, disable IP.

Out of Band Configuration Shows the following:

- *Serial Line IP Address* — SLIP allows IP to run over the console port instead of the network. SLIP allows you to use out-of-band management, either locally or remotely through a modem. SLIP operates with any valid IP address. The default is 192.168.101.1 which is the address Quick Config Manager uses.
- *SubNet Mask* — Enter the SLIP subnet mask. For a class C address, 255.255.255.0 (the default) is suitable.

If you are using SLIP and have changed any of the console port settings using VT100, ensure that Flow Control is not set to XON/XOFF, see "Connecting a Modem to the Console Port" on page 5-13.

If you require more information about SLIP, read the Internet Activities Board document RFC 155.

Router IP Address Enter the IP address of the router (if you have one) which is used by the hub to communicate with other networks.

Manager IP Address Enter the IP address of a management station that has an IP-based network management application running on it. You can configure the hub to send messages, called *traps*, to this management station.

Quick Config Manager does not have a facility to receive traps because it is a configuration tool, not a management tool.

Resetting the Hub

Resetting the hub simulates switching the hub off and on. You may want to reset the hub if you want to:

- Apply any changes made to the hub's IP configuration.
- Resets the hub's statistics counters.

CAUTION: *Performing a reset may cause some of the data being transmitted over the network to be lost.*

To reset the hub:

1. From the *Configure* menu, select *Reset*.

   Quick Config Manager asks you to confirm the reset.

2. In the confirmation dialog box, click on *OK*.

   The hub takes about 20 seconds to reset itself. You may need to select *Reset View* from the *File* menu to re-establish communication with the hub.

Initializing the Hub

Initializing the hub causes it to return to its factory default settings. You may want to do this if the hub has been previously used in a different part of your network, and its settings are incorrect for its new environment.

CAUTION: *Initializing the hub removes all configuration information such as security, resilient links and passwords. However, the IP address, subnet mask, default router, SLIP and console port information is retained to ensure you can continue management communication with the hub over the network.*

To initialize the hub:

1. From the *Configure* menu, select *Initialize*.

   Quick Config Manager asks you to confirm the initialization.

2. In the confirmation dialog box, click on *OK*.

   The hub takes about 20 seconds to initialize itself. You may need to select *Reset View* from the *File* menu to re-establish communication with the hub.

Viewing the Hub

Quick Config Manager can display a graphical representation of the hub you are managing, with:

- The ports color coded to show their condition
- The Alert LED reflecting its physical state

To display the hub:

- From the *View* menu, select *Zoom In*.

  Quick Config Manager displays a zoom view of the hub, as shown in Figure 4-4. If the zoom view is already open, it is selected.

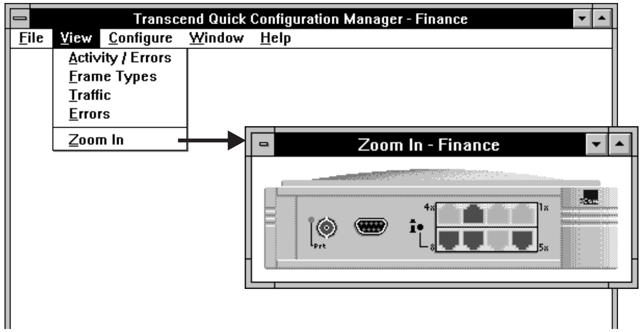


Figure 4-4 Zoom View Of The Hub

The port color coding shows these conditions:

- *Green* — Port enabled and capable of receiving and transmitting traffic
- *Red* — Port enabled and partitioned, or port enabled but the connection is lost
- *Blue* — Port disabled by management

In the Community/Polling dialog box, you can specify whether the zoom view is invoked on starting Quick Config Manager, and how often the zoom view is polled (updated). If you want to update the zoom view immediately, without waiting for a poll, select Update Zoom from the File menu.

Double-clicking on the Zoom View

You can configure information for the hub by double-clicking on the zoom view:

- If you double-click on a port, the Port dialog box is displayed. This is used to configure information for a port, see “Configuring a Port” on page 4-25.
- If you double-click on anything other than a port, the General Info dialog box is displayed. This is used to configure information for the hub, see “Displaying Information About the Hub” on page 4-13.

Displaying Information About the Hub

Quick Config Manager enables you to display detailed information about the hub. This information is stored within the hub in a list, called a *MIB* (Management Information Base). The MIB defines what information can be obtained from the hub by an SNMP network management station.

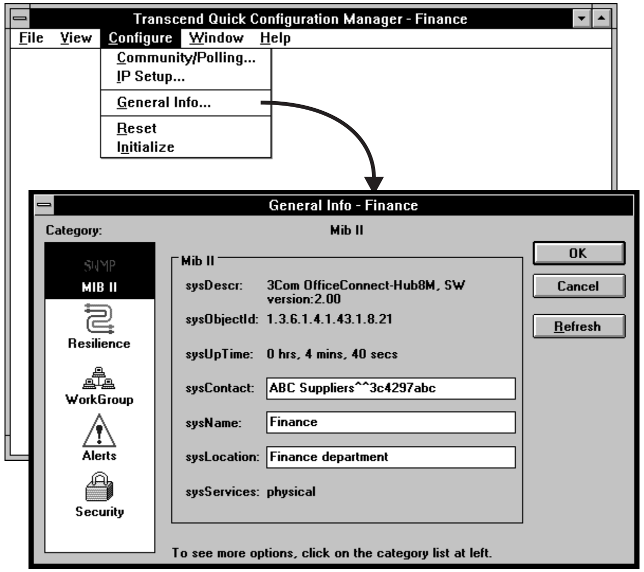
To display this information:

1 Do one of the following:

- Double-click on the graphical representation of the hub (but not on a port).
- From the *Configure* menu, select *General Info...*

2 In the General Info dialog box, select the *MIB II* category.

Quick Config Manager displays the MIB II panel, as shown in Figure 4-5.



Mib II

Mib II

sysDescr: 3Com OfficeConnect-Hub8M, SW version:2.00

sysObjectId: 1.3.6.1.4.1.43.1.8.21

sysUpTime: 0 hrs, 4 mins, 40 secs

sysContact: ABC Suppliers^^3c4297abc

sysName: Finance

sysLocation: Finance department

sysServices: physical

To see more options, click on the category list at left.

Figure 4-5 MIB II Panel

sysDescr Shows the system description supplied by the hub's Management Agent software.

sysObjectId Shows the SNMP object identifier for the hub's Management Agent software.

sysUpTime Shows the time that has elapsed since the last reset.

sysContact Provides a box for you to type the name of the person who can be contacted in the event of a problem with the hub.

sysName Provides a box for you to type the name of the hub.

sysContact and sysName use the same information as the Device Configuration fields in the IP Setup dialog box, so if you change them, the fields in the IP Setup dialog box change as well.
For information on the IP Setup dialog box, see "Giving the Hub an IP Address" on page 4-7.

sysLocation Provides a box for you to type the location of the hub.

sysServices Shows the services that the hub supports.

Refresh Refreshes the information in the panel.

Setting Up the Alert LED

The Alert LED can warn you of potential problems with your network. Quick Config Manager allows you to:

- Test the Alert LED.
- Configure the conditions that cause the Alert LED to light.
- View what conditions have caused the Alert LED to light.

You can configure the Alert LED to light for:

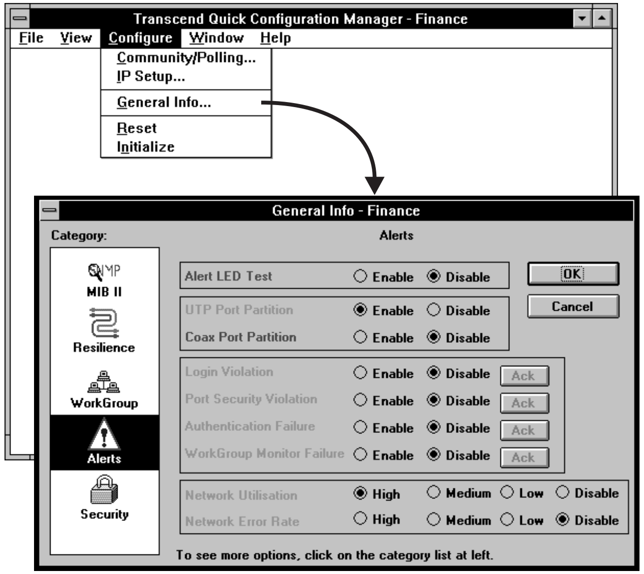
- *Incorrect configurations* — If there is a network loop due to an incorrect configuration in your network, a port partitions. The coaxial port automatically partitions if it is not used.
- *Security Violations* — If an unsuccessful login attempt occurs, or a device that is not known to your hub tries to communicate with it, a violation occurs. This may be due to someone trying to gain unauthorized access to your network.
- *Poll Failures* — If your hub has been configured to monitor a device, it periodically polls it for information. If the device fails to respond, the failure is seen by the hub.
- *Network Errors* — If the network has high volumes of communication, or there is a high amount of errors with the communication, it could be due to too many devices on your network or an incorrectly configure device.

By default, the Alert LED is configured to light if a 10BASE-T port is partitioned or if there is high network utilization (over 80%).

To configure the Alert LED:

1. Do one of the following:
   - Double-click on the graphical representation of the hub (but not on a port).
   - From the *Configure* menu, select *General Info...*
2. In the General Info dialog box, choose the *Alerts* category.

   Quick Config Manager displays the Alerts panel, as shown in Figure 4-6.



Alerts

Alert LED Test ○ Enable ● Disable

UTP Port Partition ● Enable ○ Disable

Coax Port Partition ○ Enable ● Disable

Login Violation ○ Enable ● Disable

Port Security Violation ○ Enable ● Disable

Authentication Failure ○ Enable ● Disable

WorkGroup Monitor Failure ○ Enable ● Disable

Network Utilisation ● High ○ Medium ○ Low ○ Disable

Network Error Rate ○ High ○ Medium ○ Low ● Disable

To see more options, click on the category list at left.

Figure 4-6 Alerts Panel

3 Configure the conditions for the Alert LED.

4 Click on *OK* when the Alert LED setup is complete.

If any Alert conditions are active, the conditions are displayed in red. The other conditions are displayed in green. If the active conditions are enabled, the Alert LED will be lit.

In the Alerts panel:

Alert LED Test Enabled / Disabled
Allows you to test the Alert LED. If you select Enable and click on *OK*, the Alert LED lights regardless of the true alert condition of the hub.

When you have finished your test, remember to disable to Alert LED Test. To do this, select Disable and click on OK. The Alert LED now reflects the current Alert condition of the hub.

UTP Port Partition Enabled / Disabled
Allows you to specify whether the Alert LED lights if a UTP port becomes partitioned, which happens if a network loop occurs.

If this condition is resolved after causing the Alert LED to light, the LED goes off (it stays lit if other conditions also caused it to light).

Coax Port Partition Enabled / Disabled
Allows you to specify whether the Alert LED lights if the coaxial port becomes partitioned.

If this condition is resolved after causing the Alert LED to light, the LED goes off (it stays lit if other conditions also caused it to light).

Login Violation Enabled / Disabled
Allows you to specify whether the Alert LED lights if a login violation occurs, which happens if a user attempts to log on to your hub using the VT100 screens with an invalid username/password combination three consecutive times.

If this condition caused the Alert LED to light, the LED goes off after you have acknowledged the alert by pressing the associated *Ack* button (the LED stays lit if other conditions also caused it to light).

Port Security Violation Enabled / Disabled
Allows you to specify whether the Alert LED lights if a port security violation occurs, which happens if an unauthorized device attempts to communicate through your hub.

If this condition caused the Alert LED to light, the LED goes off after you have acknowledged the alert by pressing the associated *Ack* button (the LED stays lit if other conditions also caused it to light).

Authentication Failure Enabled / Disabled
Allows you to specify whether the Alert LED lights if an authentication failure occurs, which happens if a user attempts to access information on your hub using an invalid community string.

If this condition caused the Alert LED to light, the LED goes off after you have acknowledged the alert by pressing the associated *Ack* button (the LED stays lit if other conditions also caused it to light).

WorkGroup Monitor Failure Enabled / Disabled
Allows you to specify whether the Alert LED lights if a workgroup monitor failure occurs, which happens if a remote device fails to respond to a workgroup monitor poll from your hub.

If this condition caused the Alert LED to light, the LED goes off after you have acknowledged the alert by pressing the associated *Ack* button (the LED stays lit if other conditions also caused it to light).

Network Utilization High / Med / Low / Disabled
Allows you to specify whether the Alert LED lights if a certain level of network utilization is exceeded for five seconds. The levels are:

- *High* — 80% network utilization
- *Med* — 50% network utilization
- *Low* — 12% network utilization

If this condition is resolved after causing the Alert LED to light, the LED goes off (it stays lit if other conditions also caused it to light).

Following a period of excessive network activity, the Alert LED stays lit for a short period of time.

Network Error Rate High / Med / Low / Disabled
Allows you to specify whether the Alert LED lights if a certain level of network errors is exceeded for approximately one minute. The levels are:

- *High* — 100 errors per 10000 frames
- *Med* — 10 errors per 10000 frames
- *Low* — 1 error per 10000 frames

If this condition is resolved after causing the Alert LED to light, the LED goes off (it stays lit if other conditions also caused it to light).

Monitoring

You can quickly and easily monitor your network by viewing various types of network information:

- Activity and errors
- Frame types
- Network traffic
- Network errors

The information is displayed as a graph or pie chart, and can be helpful for spotting and isolating any potential network problems you may have.

To view general information for the hub, see "Displaying Information About the Hub" on page 4-13.

Monitoring Activity and Errors Statistics

Quick Config Manager allows you to display the total network activity and errors seen by a port or the hub (all ports) in any one time period.

To display the Activity/Errors graph for a port:

1. Double-click on the port for which you want to display the Activity/Errors graph.
2. In the Port dialog box, choose the *Info* category.
3. In the Repeater Port Info panel, select the *Activity* check box.
4. Click on *OK*.

To display the Activity/Errors graph for the hub:

- From the *View* menu, select *Activity/Errors*.

Quick Config Manager displays the Activity/Errors graph, as shown in Figure 4-7.

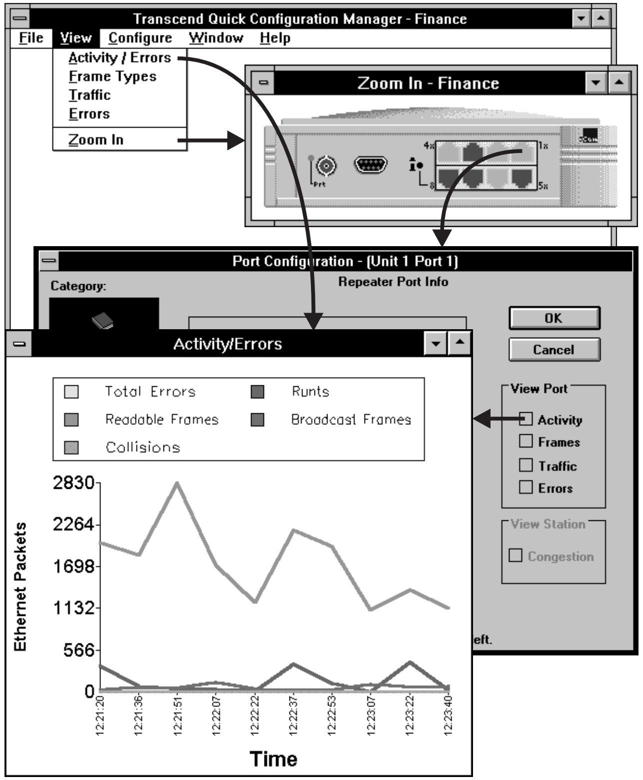


Figure 4-7 Activity/Errors Graph

Total Errors Shows the total number of errors that have occurred per poll, it should be a small percentage of the readable frames figure.

Runts Shows the number of frames received with octet counts less than the minimum legal size (512 bits), which were not involved in a collision on the segment being monitored. Runt frames are the result of collisions on other segments and are propagated around the network; this is a normal part of Ethernet operation. An excessive number of runts or collisions is an indication of congestion. You may need to consider segmenting your network (separating the busiest parts).

Readable Shows the number of frames received that are of valid length and have not suffered a collision or FCS error. Look for unusual increases in traffic rate; this can indicate a potential problem.

Broadcast Shows the number of frames received which are addressed to all devices. The number of broadcast frames is normally a small percentage of the value seen for unicast (single address) frames. A high level of broadcast frames can adversely affect network performance.

Collisions Shows the number of frames for which a transmission collision was detected. Collisions are a normal part of Ethernet operation and occur if two or more devices attempt to transmit at the same time. A sudden sustained increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic. On coaxial segments an increase in collisions can also indicate faulty cabling.

The values shown in the Activity/Errors graph are per poll period, not per second. To change the poll period, see “Accessing the Hub” on page 4-6.

Frame Types Statistics

Quick Config Manager allows you to display the total network frame types seen by a port or the hub (all ports) in any one time period. Any frames producing errors are not included, these are shown in the Activity/Errors graph, see “Monitoring Activity and Errors Statistics” on page 4-19.

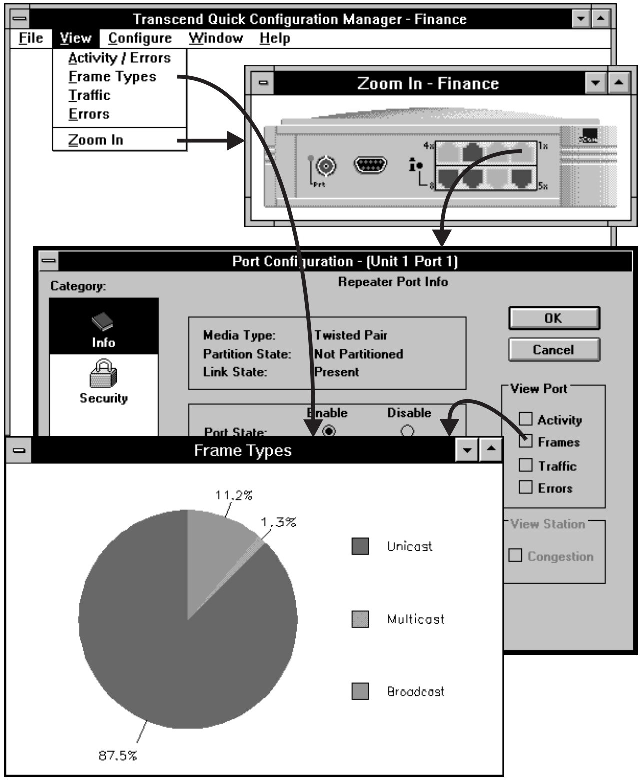
To display the Frame Types pie chart for a port:

1. Double-click on the port for which you want to display the Frame Types pie chart.
2. In the Port dialog box, choose the *Info* category.
3. In the Repeater Port Info panel, select the *Frames* check box.
4. Click on *OK*.

To display the Frame Types pie chart for the hub:

- From the *View* menu, select *Frame Types*.

Quick Config Manager displays the Frame Types pie chart, as shown in Figure 4-8.



Media Type: Twisted Pair
Partition State: Not Partitioned
Link State: Present

Port State: ● Enable ○ Disable

View Port: □ Activity ☑ Frames □ Traffic □ Errors

View Station: □ Congestion

Figure 4-8 Frame Types Pie Chart

Unicast Shows the percentage of readable frames received that are addressed to single devices.

Multicast Shows the percentage of readable frames received that are addressed to multiple devices. The total number of multicast frames is normally a small percentage of the value seen for unicast (single address) frames. A high level of multicast frames can adversely affect network performance.

Broadcast Shows the percentage of frames received which are addressed to all devices. The total number of broadcast frames is normally a small percentage of the value seen for unicast (single address) frames. A high level of broadcast frames can adversely affect network performance.

The values shown in the Frame Types pie chart are per poll period, not per second. To change the poll period, see "Accessing the Hub" on page 4-6.

Network Traffic Statistics

Quick Config Manager allows you to display the network traffic as a percentage of the total possible traffic for a port or the hub (all ports) in any one time period.

To display the Network Traffic graph for a port:

1. Double-click on the port for which you want to display the Network Traffic graph.
2. In the Port dialog box, choose the *Info* category.
3. In the Repeater Port Info panel, select the *Traffic* check box.
4. Click on *OK*.

To display the Network Traffic graph for the hub:

- From the *View* menu, select *Traffic*.

Quick Config Manager displays the Network Traffic graph, as shown in Figure 4-9. The values shown in the Network Traffic graph are the average per poll period. To change the poll period, see "Accessing the Hub" on page 4-6.

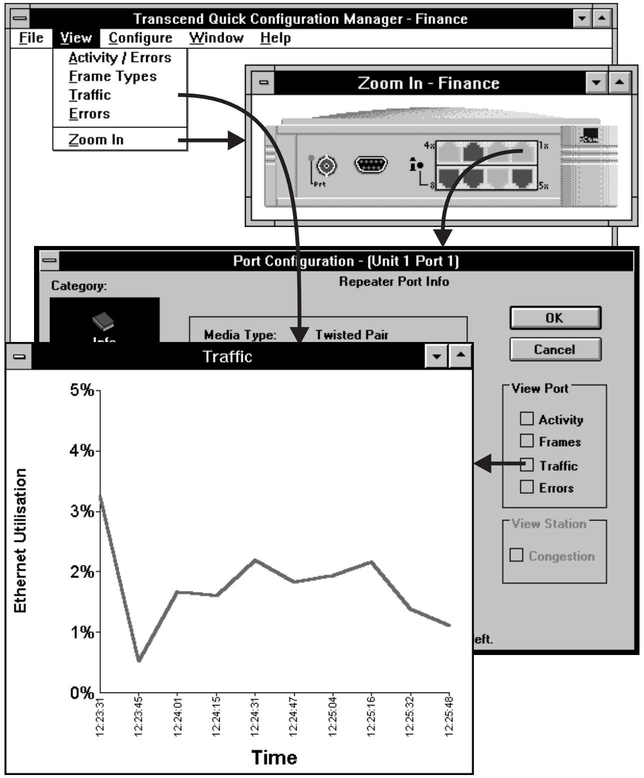


Figure 4-9 Network Traffic Graph

Network Errors Statistics

Quick Config Manager allows you to display the numbers of frames with errors seen by a port or the hub (all ports) in any one time period.

To display the Network Errors graph for a port:

1. Double-click on the port for which you want to display the Network Errors graph.
2. In the Port dialog box, choose the *Info* category.
3. In the Repeater Port Info panel, select the *Errors* check box.
4. Click on *OK*.

To display the Network Errors graph for the hub:

- From the *View* menu, select *Errors*.

Quick Config Manager displays the Network Errors graph, as shown in Figure 4-10.

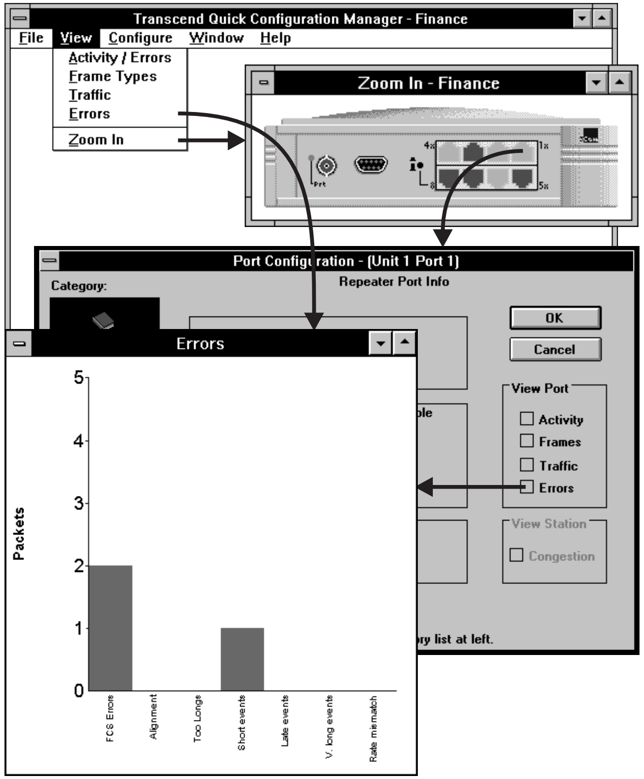


Figure 4-10 Network Errors Graph

FCS Errors Shows the number of frames received with checksum errors that do not have alignment errors. FCS errors are most likely caused by noise on the cable and should be a very small percentage of the total traffic. If it is not, change the transceivers or network adapters of devices connected to the hub to see if this eliminates the problem. FCS errors can also be caused by electrical interference from other cables or machinery.

Alignment Shows the number of frames received with alignment errors (also known as framing errors). Alignment errors should be a very small percentage of the total traffic. They are likely to be caused by a fault at the transmitting device. Locate the segment and if there is only one transmitting device (for example, fiber or 10BASE-T) change the transceiver or adapter to see if this eliminates the problem.

Too Longs Shows the number of frames received that are greater than the maximum size permitted on Ethernet (1518 octets).

Short Events Shows the number of short events received. A short event is a transmission of less than the minimum size permitted on Ethernet (64 octets). Short events can indicate externally generated noise causing problems on the network.

Check the cable routing and reroute any cabling which may be affected by other noise sources.

Late Events Shows the number of frames for which a collision was detected after the valid packet minimum time. A late event can occur if you have a Local Area Network that is longer than Ethernet standards allow (for example, more than four repeaters in series or excessively long segments).

Very Long Events Shows the number of frames that caused Jabber Lock Up protection to operate. Jabber Lock Up is when a transceiver turns itself off, if it starts uncontrollably transmitting. Isolate the source and change the transceiver or network adapter in the device to see if this eliminates the problem.

Rate Mismatch Shows the number of frames whose timing was outside the permitted range. This may indicate a non-compliant device on your network. Isolate the source and change the transceiver or network adapter in the device to see if this eliminates the problem.

The values shown in the Network Errors graph are per poll period, not per second. To change the poll period, see “Accessing the Hub” on page 4-6.

Configuring a Port

Quick Config Manager allows you to configure how individual ports operate, enabling you to introduce some simple security to your network. The hub provides more complete security which you can configure for the ports, see “Hub Security” on page 4-28.

For each port you can configure it:

- To be enabled or disabled.
- To send traps (messages) to an IP/IPX-based network management application if the port changes state, for example, the port partitions or its connection is lost.
- To learn the MAC address (hardware address) of the device connected to it.

Enabling a port allows it to repeat information to and from the network. Disabling a port prevents it from repeating information onto the network. We recommend that you disable any unused ports to prevent unauthorized use.

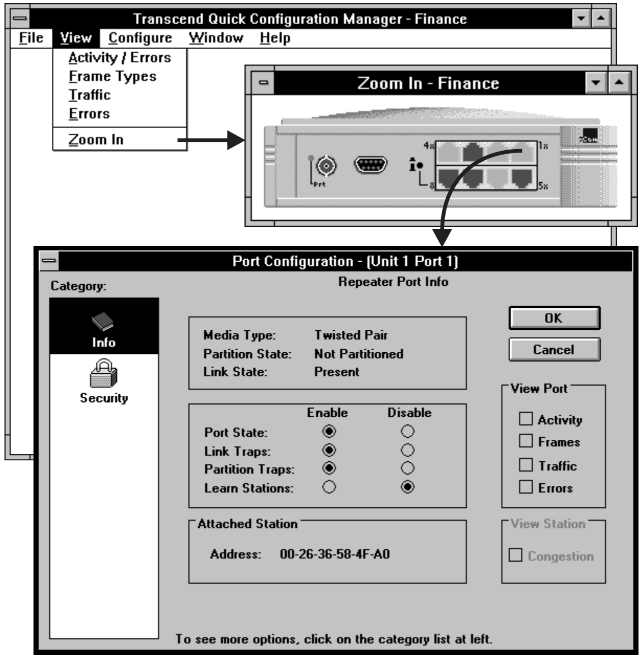
You can configure a port so that it sends a trap to a network management application when the status of the link changes (for example, if a device is connected to or disconnected from the port), or when the port partitions. You can also configure a port to store the source address of frames received by the port, this enables you to detect which devices are attached to each port of the hub.

To configure a port:

1. From the *View* menu, select *Zoom In* to display the representation of the hub.
2. Double-click on the port you want to configure.
3. In the Port Configuration dialog box, choose the *Info* category.

   Quick Config Manager displays the Repeater Port Info panel, as shown in Figure 4-11.
4. In the Repeater Port Info panel, select either Enable or Disable for Port State.

If the port is part of a resilient link, you cannot enable or disable the port. You must first delete the resilient link, see “Resilience” on page 4-33.


Transcend Quick Configuration Manager - Finance
File View Configure Window Help
Activity / Errors
Frame Types
Traffic
Errors
Zoom In
Zoom In - Finance
Port Configuration - [Unit 1 Port 1]
Category:
Info
Security
OK
Cancel

Repeater Port Info

Media Type: Twisted Pair
Partition State: Not Partitioned
Link State: Present

	Enable	Disable
Port State:	●	○
Link Traps:	●	○
Partition Traps:	●	○
Learn Stations:	○	●

Attached Station
Address: 00-26-36-58-4F-A0

View Port
☐ Activity
☐ Frames
☐ Traffic
☐ Errors

View Station
☐ Congestion

To see more options, click on the category list at left.

Figure 4-11 Repeater Port Info Panel

5 Select either Enable or Disable for Link Traps, Partition Traps, and Learn Stations.

6 Click on *OK*.

In the *Repeater Port Info* panel:

Media Type Shows the type of media connected to the port.

Partition State Shows whether the port is on and repeating traffic, or has been automatically isolated (partitioned). If the port has partitioned check the cabling at both the port and any devices connected to the port, and check for network loops.

Link State Shows the state of the link for a twisted pair (10BASE-T) port.

Port State Enabled / Disabled
Selects whether the port can repeat information to and from the network.

Link Traps Enabled / Disabled
Selects whether a trap is sent to an IP/IPX-based network management application if the link state changes.

Partition Traps Enabled / Disabled
Selects whether a trap is sent to an IP/IPX-based network management application if the partition state changes.

Learn Stations Enabled / Disabled
Selects whether the source address of received frames is learned.

Attached Station Shows the MAC address of the device attached to this port (the last device to transmit to this port).

The check boxes in the View Port box enable you to display statistics for the port and are described in "Monitoring" on page 4-18.

The View Station box is always disabled for Quick Config Manager.

Hub Security

The OfficeConnect Hub 8/TPM provides flexible communication between your workstations and other network equipment. It is a good idea to configure security for the hub to protect your network from unwanted communications.

Security can be performed at two levels:

- *Port* — Configure security for an individual port.
- *Hub* — Configure security for one or more ports at a time.

The way you set up your security depends on what you want to do. For example, if you have one device connected to a specific port, you would manage at **port** level to secure that connection. If you have several devices that you want to connect to any of a number of ports, you would manage at **hub** level to secure that connection.

If you simply want to disable a port, see "Configuring a Port" on page 4-25.

3Com's security is very advanced but easy to set up. It works by learning in a number of ways what devices are communicating through its ports. You can configure the hub to react in two ways:

- *Disconnect Unknown Device (DUD)* — If the hub detects a communication from an unknown device at a port, it can disable that port to prevent further communication.
- *Need To Know (NTK)* — If a frame is to be forwarded from a port, the destination address of the frame is checked and if it does not match the device learnt for that port, the frame is scrambled to prevent the communication from being intercepted.

Configuring Security at Port Level

To configure security for a port:

1 From the *View* menu, select *Zoom In* to display the representation of the hub.

2 Double-click on the port for which you want to configure security.

Quick Config Manager displays the Port Configuration dialog box.

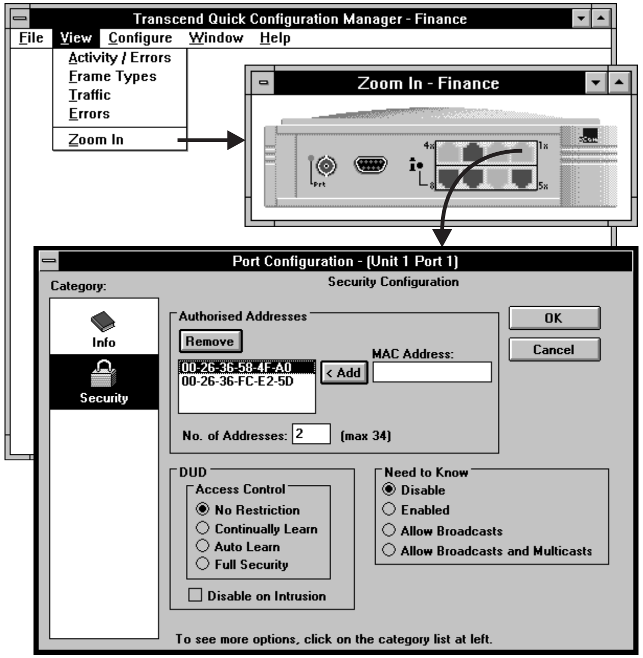
3 In the Port Configuration dialog box, select the *Security* category.

Quick Config Manager displays the Port Security Configuration panel, as shown in Figure 4-12.

In the Port Security Configuration panel at port level:

Authorized Addresses Shows the following:

- *No. of Addresses* — Displays the number of addresses that can be authorized for this port. The list above it shows any addresses already configured for this port.



Port Configuration - [Unit 1 Port 1]

Category: Info, Security

Security Configuration

Authorised Addresses

Remove

00-26-36-58-4F-A0
00-26-36-FC-E2-5D

< Add

MAC Address:

No. of Addresses: 2 (max 34)

OK

Cancel

DUD

Access Control

● No Restriction
○ Continually Learn
○ Auto Learn
○ Full Security

□ Disable on Intrusion

Need to Know

● Disable
○ Enabled
○ Allow Broadcasts
○ Allow Broadcasts and Multicasts

To see more options, click on the category list at left.

Figure 4-12 Port Security Configuration Panel

- *MAC Address* — Allows you to enter the MAC address for a device to be authorized to transmit through this port. When you have typed the MAC address, click on *<Add*. Use the format xx-xx-xx-xx-xx-xx for the MAC address.
- *<Add* — Adds the MAC address to the Authorized addresses list.
- *Remove* — Removes the selected address or addresses from the Authorized Address list.

DUD (Disconnect Unknown Device) Allows you to configure the learning and security mode of the port:

- *No Restriction* — Disables all security and learning features.
- *Continually Learn* — The port learns the MAC addresses of the devices transmitting to this port and stores them in its address table. The maximum number of addresses learned by the ports is determined by the value shown in the No. of Addresses field. When the table is full, the port continues to learn new addresses, overwriting the addresses it learned previously.

  The port never automatically switches to full security (for example Auto Learn), you have to do this manually. While learning, packets received on a port are not repeated out of the other ports.
- *Auto Learn* — The port learns the MAC addresses of the devices transmitting to this port and stores them permanently in its address table. The maximum number of addresses learned by the ports is determined by the value shown in the No. of Addresses field. When the table is full, the port automatically switches to Full Security mode and no other address are allowed to connect to this port. While learning, packets received on a port are not repeated out of the other ports.
- *Full Security* — Learning is disabled and only the addresses entered as authorized addresses for this port are allowed to transmit. If an unauthorized address is detected, a trap will be sent (if traps are configured) to an IP/IPX-based management station, and the port is disabled (if *Disable on Intrusion* is selected).

- *Disable on Intrusion* — Compares the source address of all frames received on the port to the authorized addresses for that port. If the source address of the incoming frame does not match the authorized addresses for this port, the port is disabled to prevent communication. This option is only valid when *Full Security* has been selected.

Need To Know Allows you to configure which frames are forwarded to the selected port. If the port does not support configurable Need To Know, these options are grayed out:

- *Disabled* — All frames are forwarded.
- *Enabled* — The port examines the destination address of the frame. If it matches an authorized address for the port it is forwarded. If it does not, it is scrambled, so it can't be read.
- *Allow Broadcasts* — In addition to Enabled, allows broadcast frames to be transmitted to the port.
- *Allow Broadcasts and Multicasts* — In addition to Enabled, allows broadcast and multicast frames to be transmitted to the port.

When you click on OK, the operation may fail for one of the following reasons:

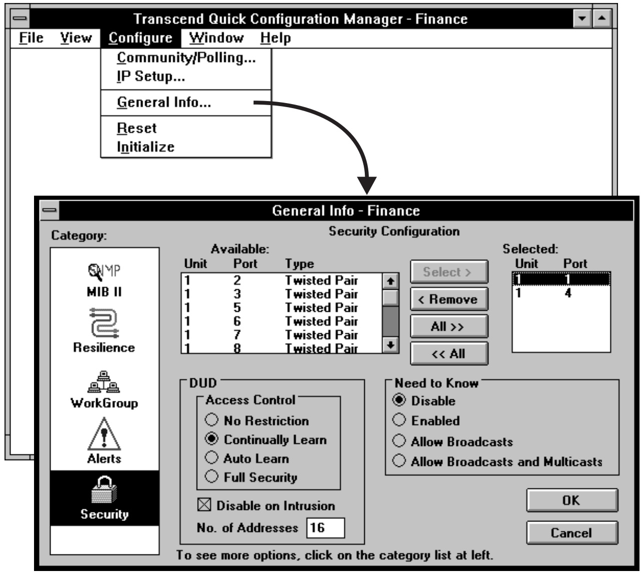
- The operation has timed out.
- An Invalid MAC address (in other words, Multicast or Broadcast address) has been entered into the list of authorized addresses.
- There is a duplicate address on another port.

If the address is on another port already and DUD is set to Full Security or Autolearn, you must remove the address from the other port before it can be assigned to the current port.

Configuring Security at Hub Level

To configure security for a hub:

1. Do one of the following:
   - Double-click on the graphical representation of the hub (but not on a port).
   - From the *Configure* menu, select *General Info...*
2. In the General Info dialog box, choose the *Security* category.



Security Configuration

Available:

Unit	Port	Type
1	2	Twisted Pair
1	3	Twisted Pair
1	5	Twisted Pair
1	6	Twisted Pair
1	7	Twisted Pair
1	8	Twisted Pair

Selected:

Unit	Port
1	1
1	4

DUD

Access Control

○ No Restriction
● Continually Learn
○ Auto Learn
○ Full Security

☒ Disable on Intrusion

No. of Addresses 16

Need to Know

● Disable
○ Enabled
○ Allow Broadcasts
○ Allow Broadcasts and Multicasts

To see more options, click on the category list at left.

Figure 4-13 Security Configuration Panel

Quick Config Manager displays the Security Configuration panel, as shown in Figure 4-13.

3 Configure the security features for each port.

4 Click on *OK* when the security setup is complete.

In the Security Configuration panel at hub level:

- *Available* — This lists the hub's ports, identifying them by port number and media type. Click on a port to select it from the list or perform a multiple selection.
- *Selected* — Shows the ports selected to be configured. Click on a port to select it from the list or perform a multiple selection.
- *Select>* — Adds the selected ports in the Available list to the Selected list.
- *<Remove* — Removes the selected ports from the Selected list to the Available list.
- *All>>* — Adds all the available ports to the Selected list.
- *<<All* — Removes all the selected ports from the Selected list.

DUD and **Need To Know** are the same as for port level, see "Configuring Security at Port Level" on page 4-29.

Resilience

You can make your network more robust by adding *resilience* to it.

When a link fails, as shown in Figure 4-14, all communication between equipment on each side of the link is lost. It would be very inconvenient for a manager to physically reinstate the network immediately and important communication might be lost.

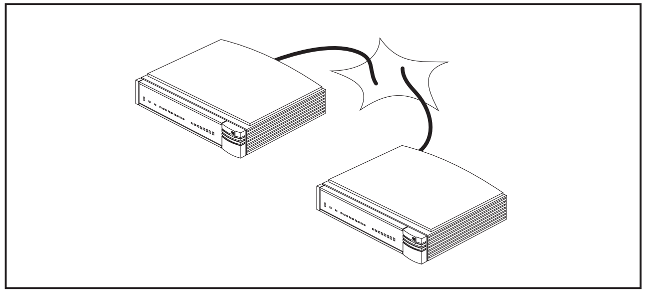


Figure 4-14 A Failed Link Between Two Hubs

If a spare link could automatically pick up when the broken link failed, the network would appear to function normally to the user. At worst, a few packets would be corrupted or lost.

This is the concept of resilience. One link is on standby (called the *standby* link) waiting to take over if another link (called the *main* link) fails, as shown in Figure 4-15. This pair is called a *resilient link pair*.

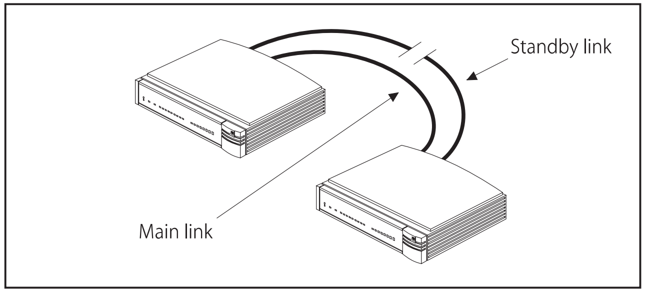


Figure 4-15 A Resilient Link Pair

Resilient Links are available over twisted pair media (10BASE-T) because it carries a link test pulse which is used to decide whether the main link has failed and the standby link should take over. However, there is no such link signal over coaxial media (10BASE-2), so you cannot set up resilient links using the hub's 10BASE-2 (Coax) port.

If you have more than two hubs there are a number of ways you can use resilience when linking them. Remember to follow hub connection requirements; always connect an MDIX port to an MDI port, setting the MDIX switch as appropriate, see "Connecting Hubs Using 10BASE-T" on page 2-10.

When your network is in use, the hub that has been used to set up the resilient link pair, monitors the state of both the main link and the standby link. If the main link fails, the standby link becomes active. If the fault with the main link is solved, the standby link stays active and the main link acts like a standby link.

You can use management to view the status of your links, and to send *traps* (messages) to an IP/IPX-based network management application, if anything changes.

Setting Up a Resilient Link Pair

To set up a resilient link pair, you need to manage the hub that both links in the pair are connected to. You can set up to 4 resilient link pairs for the hub.

When you set up your resilient link pair, you only need to specify the ports that the main link and standby link are connected to.

Resilient Link Rules

Always follow these rules when setting up a resilient link pair:

- Configure the resilient link pair at only one end of the link. In other words, only one hub controls each resilient link pair you set up.
- Each resilient link pair can only have one main link and one standby link.
- Each link must not belong to more than one resilient link pair.
- For a port that is part of a resilient link pair:
  - Do not disable the link pulse generation.
  - Do not enable security for the port.

CAUTION: *Remember that you must always follow the hub connection requirements when linking hubs together, which involves the use of port 8 and the MDI/MDIX switch.*

If port 8 is already in use, you may need to use special crossover cabling for any further links you wish to make. Crossover cables allow you to make a connection between two MDIX ports. Contact your supplier for information on doing this.

To set up a resilient link pair:

1 Disconnect the hub which is to provide the standby port from the network. We recommend you do this, even though it is possible to set up links while still connected, to avoid loops being formed accidently.

2 Do one of the following:

- Double-click on the graphical representation of the hub (but not on a port).
- From the *Configure* menu, select *General Info...*

3 In the General Info dialog box, choose the *Resilience* category.

The Resilience Links panel is displayed.

4 In the Resilience Links panel, click on *Create*.

Quick Config Manager displays the Create Resilient Pair dialog box, as shown in Figure 4-16.

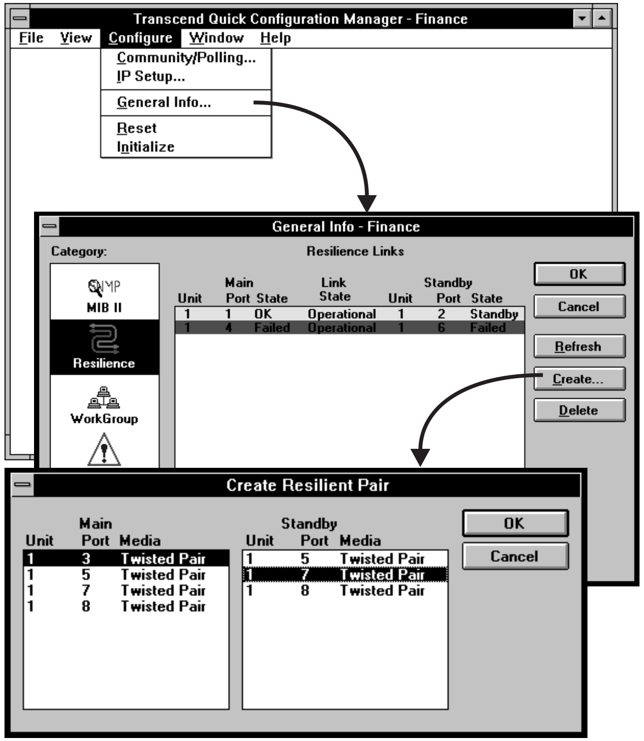
5 In the Create Resilient Pair dialog box, choose the port for the main link, followed by the port for the standby link.

6 Click on *OK*.

7 Reconnect the hub with the standby port on it to the network.

When you have created a resilient link pair, it is added to the table and is color-coded as follows:

- *Green* — Both Main link and Standby link are OK.
- *Yellow* — One of the links is OK, the other has failed.
- *Red* — Both Main link and Standby link have failed.



Resilience Links

Unit	Main Port	Main State	Link State	Standby Unit	Standby Port	Standby State
1	1	OK	Operational	1	2	Standby
1	4	Failed	Operational	1	6	Failed

Main

Unit	Port	Media
1	3	Twisted Pair
1	5	Twisted Pair
1	7	Twisted Pair
1	8	Twisted Pair

Standby

Unit	Port	Media
1	5	Twisted Pair
1	7	Twisted Pair
1	8	Twisted Pair

Figure 4-16 Create Resilient Pair Dialog Box

In the Resilience Links panel:

Main Port Shows the port number of the main link.

Standby Port Shows the port number of the standby link.

Link State Shows whether the resilient link pair is operational or not. When operational either the main port or the standby port can repeat traffic.

Main State, Standby State Shows whether the main or the standby link is the active link in the resilient link pair.

Refresh Refreshes the information in the panel.

Create Displays a dialog box which you can use to create new resilient link pairs, by choosing the main and standby links in the resilient link pair.

Delete Removes the resilient link pair from the table when an entry in the resilience table is selected. If you delete an entry in the resilience table, the current active link remains enabled and the current standby link is cancelled.

If the main link fails, the standby link becomes active. If the fault with the main link is solved, the standby link stays active and the main link acts like a standby link. You can swap the links around using management.

Using the Hub to Monitor Other Devices

Your hub can be used to monitor other devices on your network, and to notify an IP/IPX-based network management application should a problem occur with a device attached to it. The hub notifies the IP/IPX-based network management application by sending SNMP traps (messages) to it.

If you have a large network with many devices, this feature allows you to distribute device monitoring among those managed devices on your network, easing the load on the IP/IPX-based network management application.

This facility also allows you to monitor devices that are otherwise not directly manageable, such as workstations. Any device with an IP or IPX address can be monitored.

To add a device for the hub to monitor:

1. Do one of the following:
   - Double-click on the graphical representation of the hub (but not on a port).
   - From the *Configure* menu, select *General Info...*

2 In the General Info dialog box, choose the *WorkGroup* category.

3 In the WorkGroup Monitor panel, click on *Add*.

Quick Config Manager displays the Add Remote Poll dialog box, as shown in Figure 4-17.

4 In the Add/Edit Remote Poll dialog box, enter the IP or IPX address of the device that you want the hub to poll.

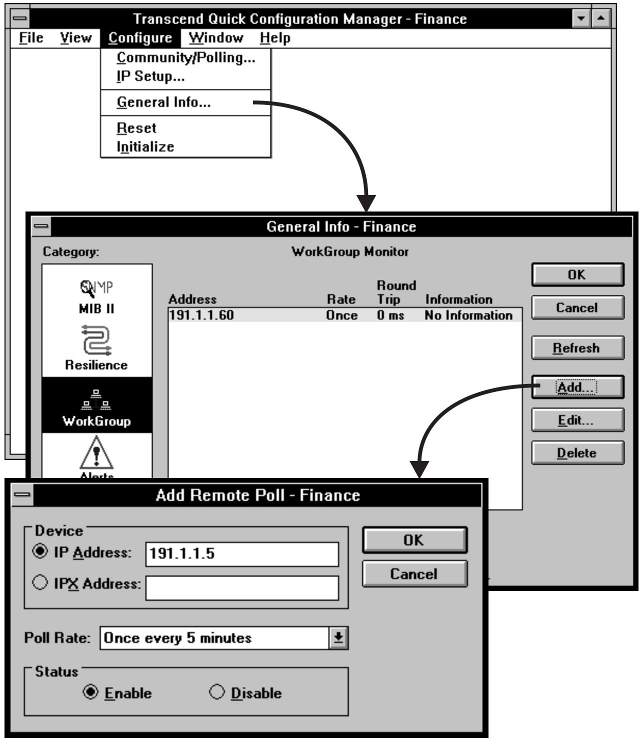
5 Choose the rate at which the device is to be polled.

If the device is critical to the performance of your network, select a frequent rate. If the device is not important or on a remote network you can select a less frequent rate.

6 Select whether polling of this device is to be enabled or disabled.

You can have up to 10 polling session entries for the hub (poll 10 different devices), all of which can be enabled. If you do not want to poll a device now but want to keep its information for future use, you can simply disable it by selecting Disable.

7 Click on *OK*.



Address	Rate	Round Trip	Information
191.1.1.60	Once	0 ms	No Information

Device
● IP Address: 191.1.1.5
○ IPX Address:

Poll Rate: Once every 5 minutes

Status
● Enable ○ Disable

Figure 4-17 Add Remote Poll Dialog Box

When you have added a device to the WorkGroup Monitor table, its entry is color-coded:

- *Green* — Device being polled and communicating.
- *Red* — Device being polled but is not communicating.
- *Blue* — Device not being polled by the hub.

In the WorkGroup Monitor panel:

Address Shows the addresses of the polled devices.

Rate Shows the frequency at which the device is polled.

Round Trip Shows the time taken for the device to respond to the last poll.

Information Shows the number of routers through which the hub communicates with the device or any information gathered during the poll.

You can edit or delete a Remote Poll by selecting it from the panel and clicking on the appropriate button.

Additional Management

If you want to perform any of the following additional management, use the VT100 screens, refer to Chapter 5:

- View the MAC address
- Specify IPX information
- Connect a modem to the console port
- Create new users, with different community strings, and disable different access methods
- Poll a remote device to see if it is working
- View the versions of the hub’s internal software and hardware
- Download new software to the hub

5 ADDITIONAL MANAGEMENT USING VT100

This chapter describes the additional management tasks you can perform using VT100®. For an overview of the management you can perform and the different ways you can make a management connection to the hub, see Chapter 3.

Only the additional management screens are described in this chapter. For information on what the other screens do, refer to the corresponding Quick Config Manager screens in Chapter 4. The VT100 Screen Map on page 5-5 includes these references.

This chapter starts with an overview of the VT100 user interface. A map of all the screens is given, to help you to access any chosen screen.

In the descriptions of the options given in this chapter, the default values are underlined.

VT100 User Interface

We suggest you read through this section before you use the hub's VT100 facility for the first time. Afterwards, you should only need it for reference.

Screens

Screens are divided into three main areas:

- The header area, at the top of the screen, displays a title which tells you the subject of the screen.
- The main part of the screen shows management information.
- The message area, at the bottom of the screen, is used to display information and error messages.

The displayed screens may not be identical to those illustrated in this chapter. The contents of screens depend on your access level. Access levels are described in "Logon" on page 5-7.

Screen Components

The main part of a typical screen contains several different types of item. This table gives an example of each component, and explains its use:

Component	Description
`◆Enabled◆` *Choice Field*	Text enclosed in markers is a list, from which you can select one option only. To cycle through the options, press [Space].
`[005634]` *Entry Field*	Text enclosed in square brackets on the screen is an Entry Field. Entry Fields allow you to enter data from the keyboard, which may be text, decimal or hexadecimal data. In some cases there is a default entry. To replace the default entry, simply type in the new value over it. Password entry fields are hidden. Anything typed is not shown on the screen. To delete a single character, use [Delete] on a VT100 terminal or [Backspace] on a PC.
`Address:` *Read-only information*	Text not enclosed in markers or square brackets is information that you cannot change.
`OK` *Button*	Text for a button is shown in upper-case letters. A button performs an action. A menu screen such as the Main Menu consists of a number of buttons arranged in a column. Other screens have a row of buttons at the bottom. To select a button, move the cursor to the button and press [Return]. The OK and CANCEL buttons appear on many screens. OK updates the hub according to the data in the fields of the screen, then returns you to the previous screen. CANCEL returns you to the previous screen without applying any changes

`monitor`
`manager`
`security`
List Box
	A list box allows you to select one or more items from a list. Selected items are indicated by an asterisk (*) next to the item.
	To select a single item, move the cursor (using the arrow keys) until the item is highlighted, then press [Return].
	To select more than one item: for each item, move the cursor until the item is highlighted, then press [Space] to select the item (pressing [Space] again deselects the item). When all the desired items are selected, press [Return].

Special Keystrokes

As well as the keystrokes previously described, there are several other keystrokes for controlling the VT100 interface. These keystrokes allow you to move the cursor around the screen, enter information and move from one screen to another:

[Tab]	Moves the cursor from one field to the next.
[Ctrl]+[B]	Moves the cursor to the next button.

When you have finished entering or changing data, [Ctrl]+[B] is very useful for skipping over the remaining fields.

[Ctrl]+[P]	Returns you to the previous screen without actioning any inputs.
[Ctrl]+[R]	Refreshes the screen.
[Ctrl]+[K]	Displays a list of the possible keystrokes.

If you are using Telnet or a terminal emulation program, you may find that some control keys do not operate, or that they activate other functions. The Windows terminal emulator uses [Ctrl]+[H] as backwards deletion, whereas others use it for backward cursor movement. Consult the manual accompanying your Telnet or terminal emulation software before using the control keys.

Repeater, Unit and Port Screens

There are three levels at which you can manage the hub using VT100:

- *Repeater* — If you manage at Repeater level, you are managing or viewing the device as a whole. Any stackable products, for example 3Com's SuperStack® range, can be logically stacked so that all the products form a single, logical repeater.
- *Unit* — If you manage at Unit level, you are managing or viewing the hub.
- *Port* — If you manage at Port level, you set up parameters and examine statistics for individual ports. This allows you to manage individual users or small workgroups.

3Com's OfficeConnect® range can be physically stacked but not logically stacked. Each unit remains a separate repeater regardless of how it is connected to other OfficeConnect units. Therefore, managing the hub at *Repeater* level is the same as managing it at *Unit* level.

Screen Map

Figure 5-1 shows how the menus and screens are related to each other. The numbers denote the pages in this chapter where the screen's description can be found.

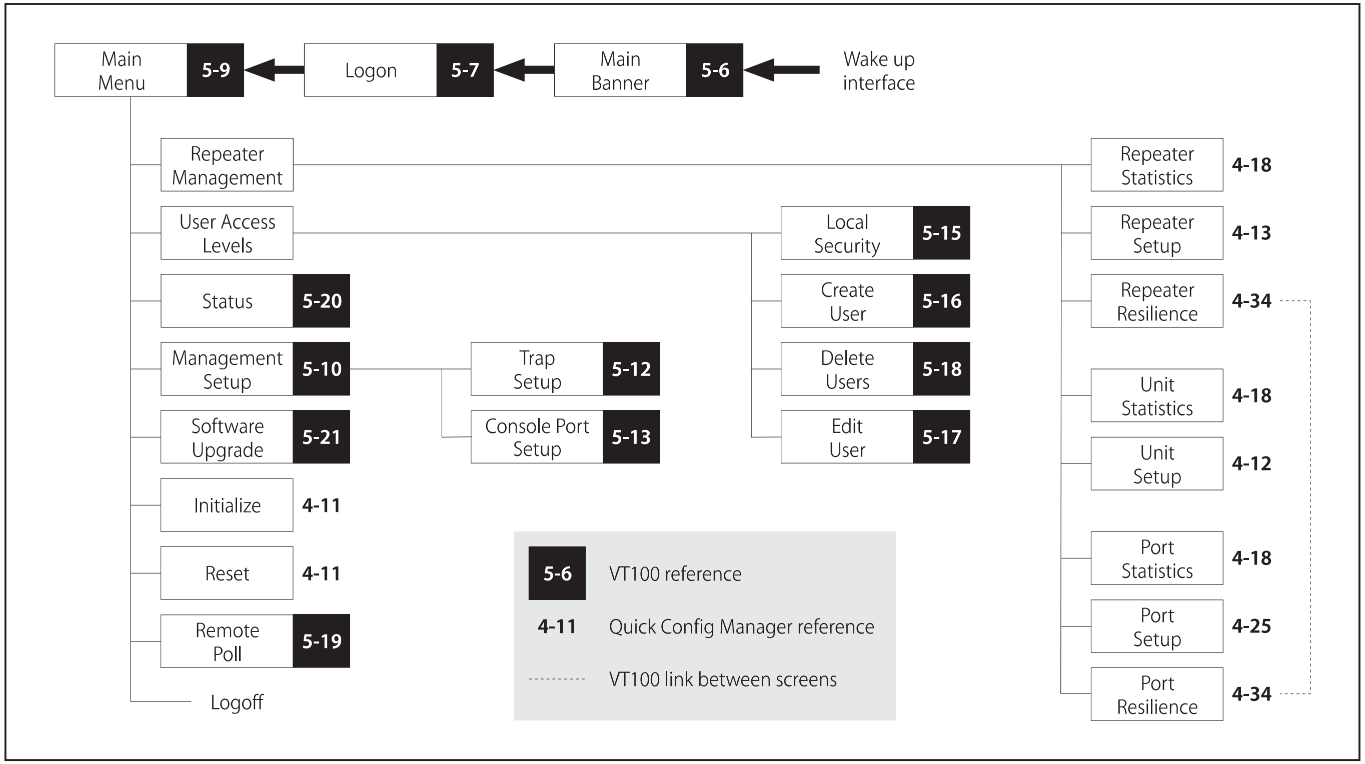


Figure 5-1 VT100 Screen Map

Getting Started

This section explains logging on to the VT100 management facility, displaying the main menu and logging off.

Main Banner

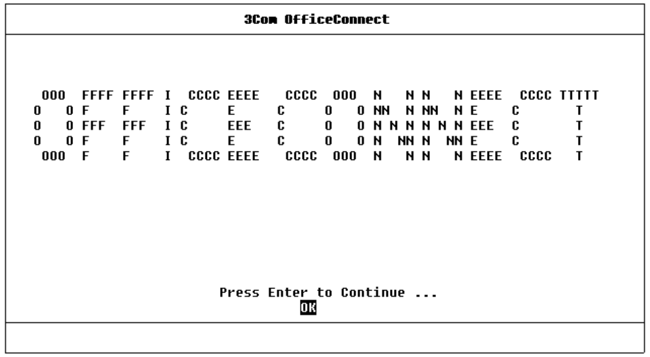
If you are using a VT100 terminal connected (directly or through modems) to the console port, you need to perform the wake-up procedure. To do this, press [Return][Return] at the terminal.

By default, the hub automatically configures the baud rate of its console port to operate with the connected terminal or modem, provided the parity, stop bits and character size are identical to the connected terminal or modem.

If you are using Telnet or SLIP, the wake-up procedure is performed automatically.

When the wake-up procedure is successfully completed, the main banner is displayed, as shown in Figure 5-2.

Press [Return] to display the Logon screen.



```
                              3Com OfficeConnect

 OOO  FFFF FFFF I  CCCC EEEE   CCCC  OOO  N   N N   N EEEE  CCCC TTTTT
O   O F    F    I C     E     C     O   O NN  N NN  N E    C       T
O   O FFF  FFF  I C     EEE   C     O   O N N N N N N EEE  C       T
O   O F    F    I C     E     C     O   O N  NN N  NN E    C       T
 OOO  F    F    I  CCCC EEEE   CCCC  OOO  N   N N   N EEEE  CCCC   T

                           Press Enter to Continue ...
                                      OK
```

Figure 5-2 Main Banner Screen

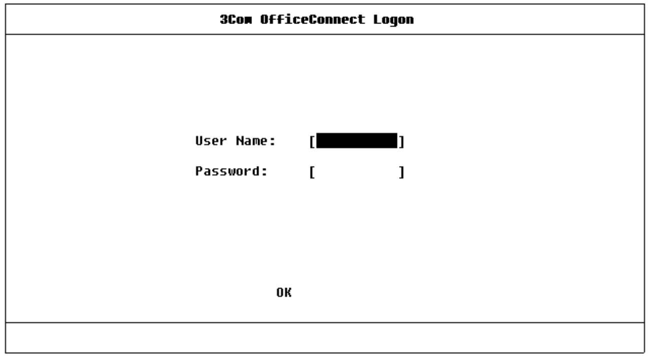
If you cannot see the main banner or it displays incorrectly, it may be that:

- *Your terminal is not configured as a VT100 terminal. Check that your terminal is set up to operate with the same parameters that the hub's console port uses. The console port's autoconfigure option only operates if your terminal uses correct parameters. The maximum speed is 19200 baud. For information on the console port, see "Connecting a Modem to the Console Port" on page 5-13.*
- *Autoconfigure is disabled.*
  If you are unable to obtain the banner screen, it is possible that the autoconfigure option has been disabled. Check the configuration of the terminal.

If you cannot resolve the problem, refer to "Problems When Using VT100" on page 6-3 for more problem solving information.

Logon

You must enter your user name and password in the Logon screen, as shown in Figure 5-3, before you can use the management facility.



```
                 3Com OfficeConnect Logon

            User Name:    [          ]
            Password:     [          ]

                   OK
```

Figure 5-3 Logon Screen

If you are logging on for the first time (after installation or initialization), use one of the default user names and passwords shown in the following table. The user name to use depends on which access level you require:

User Name	Default Password	Access Level
monitor	monitor	Monitor — You can access but not change the operational parameters of the hub.
manager	manager	Manager — You can change the operational parameters of the hub but cannot add or delete users, download software or initialize the hub.
security	security	Security — You can access all the screens and change all manageable parameters.

At the earliest opportunity, the system manager should change the passwords for the default users. The system manager needs to log on as 'manager' and 'monitor' to change their passwords. For information on how to change a password, see "Editing Users" on page 5-18.

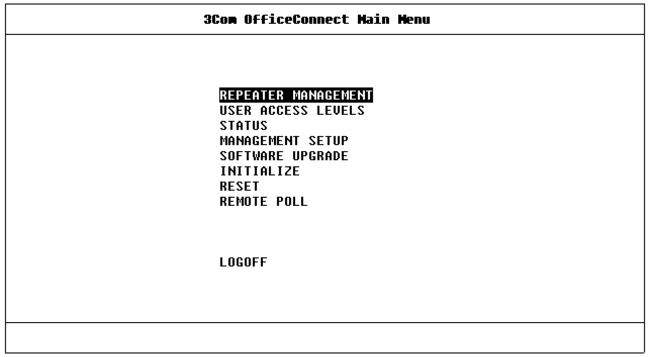
Initializing the hub returns the passwords to their default values.

If you are not logging on as one of the default users, your system manager has assigned you a user name and password. The user name determines which of the three access levels (monitor, manager or security) you have.

The user name and passwords are case sensitive. To log on to the facility, enter your user name and password in the appropriate fields and select *OK*. The Main Menu screen is displayed.

Main Menu

The Main Menu, as shown in Figure 5-4, is used for accessing the various VT100 screens.



```
3Com OfficeConnect Main Menu

REPEATER MANAGEMENT
USER ACCESS LEVELS
STATUS
MANAGEMENT SETUP
SOFTWARE UPGRADE
INITIALIZE
RESET
REMOTE POLL

LOGOFF
```

Figure 5-4 Main Menu

If you are using the management facility for the first time, we suggest that you:

- Set up logons for any other users and assign each user an appropriate security level. See “Configuring Local Security” on page 5-15.
- Assign new passwords for the default users. See “Editing Users” on page 5-18.

To carry out a particular management task, scroll to the relevant option and press [Return]. This chapter describes the screens which perform management tasks that Quick Config Manager does not.

Logoff

If you have finished using the facility, select the *Logoff* option from the bottom of the Main Menu. If you accessed the facility using a Telnet session or modem connection, the connection is closed automatically.

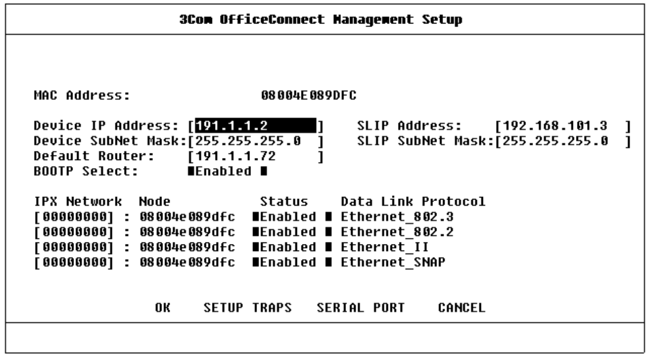
Auto Logout

There is a built-in security timeout on the VT100 interface. If you do not press any keys for three minutes, the management facility warns you that the inactivity timer is about to expire. If you do not press a key within 10 seconds, the timer expires and the screen is locked (any displayed statistics continue to be updated, however). When you next press any key, the display changes to the Auto Logout screen, which requests that you enter your password again. If entered correctly, you are returned to the screen that was previously active. If entered incorrectly, you are returned to the Logon screen.

Configuring and Viewing Setup Information

The Management Setup screen, as shown in Figure 5-5, is used to configure IP, IPX and SLIP parameters for the hub. This screen also provides access to other screens for you to set up traps and console port parameters.

If you have no previous knowledge of IP, refer to Appendix B for more information.



```
                    3Com OfficeConnect Management Setup

MAC Address:                08004E089DFC

Device IP Address: [191.1.1.2         ]    SLIP Address:    [192.168.101.3  ]
Device SubNet Mask:[255.255.255.0   ]    SLIP SubNet Mask:[255.255.255.0  ]
Default Router:    [191.1.1.72      ]
BOOTP Select:      ■Enabled ■

IPX Network  Node           Status    Data Link Protocol
[00000000] : 08004e089dfc  ■Enabled ■ Ethernet_802.3
[00000000] : 08004e089dfc  ■Enabled ■ Ethernet_802.2
[00000000] : 08004e089dfc  ■Enabled ■ Ethernet_II
[00000000] : 08004e089dfc  ■Enabled ■ Ethernet_SNAP
```

Figure 5-5 Management Setup Screen

MAC Address The MAC address of the hub. This cannot be changed.

Device IP Address If using IP, you need to enter a unique IP address for the hub, see “IP Addresses” on page B-1. You may use the BOOTP facility (see the BOOTP Select field description) if your network has a BOOTP server, or enter it manually. If you change the device IP address, you must reset the hub to effect the change.

CAUTION: *To ensure that Quick Config Manager can always communicate with the hub, the IP subnet 192.168.101.x is permanently assigned to the SLIP port in addition to the user configurable SLIP address. Do not use this subnet for your Ethernet (network).*

Device SubNet Mask If using IP, enter a suitable subnet mask. BOOTP does this automatically. For a class B IP address, 255.255.0.0 is suitable. If you change this field, reset the hub to effect the change.

Default Router If necessary, enter the IP address of the default router on your network. BOOTP does this automatically. If you change this field, reset the hub to effect the change.

SLIP Address SLIP (Serial Line Internet Protocol) allows IP to run over the console port instead of the network. SLIP allows you to use out-of-band Telnet or SNMP management, either locally or remotely through a modem. SLIP operates with any valid IP address. The default is 192.168.101.1 which is the address Quick Config Manager uses. If you change this field, reset the hub to effect the change.

CAUTION: *Changing the SLIP address and SLIP subnet mask can prevent Quick Config Manager from accessing the hub.*

If you require more information about SLIP, read the Internet Activities Board document RFC 155.

SLIP SubNet Mask Enter a suitable subnet mask. For a class C address, 255.255.255.0 (the default setting) is suitable. If you change this field, reset the hub to effect the change.

If you are using SLIP, ensure that Flow Control is not set to XON/XOFF. For information on the console port, see "Connecting a Modem to the Console Port" on page 5-13.

BOOTP Select Enabled / Disabled
When enabled, BOOTP allows you to download the IP address, the SubNet Mask, and the Router IP address from a BOOTP server on your network. When operative, BOOTP checks that a valid IP address is not installed before sending out requests for the data.

It continues sending requests for data until one of three conditions is satisfied:

- BOOTP is disabled
- A valid BOOTP reply is received
- You enter the address manually

When the IP parameters have been received, the hub resets automatically.

The following four fields are used for IPX addressing:

IPX Network This field shows the address of the network for this protocol. This address is learned automatically from the local IPX router or NetWare File Server, and you should not need to change it.

Node This field shows the node address of the hub, which is learned automatically.

Status Enabled / Disabled
This field shows whether the data link protocol is enabled. Choose Disabled if you wish to prevent access for any reason, such as security considerations.

Data Link Protocol This field shows the name of the IPX data link layer protocol.

OK Press [Return] when the *OK* button is highlighted to action your selections for this screen. You are returned to the Main Menu.

If you have changed the parameters, you need to reset the hub to effect the changes.

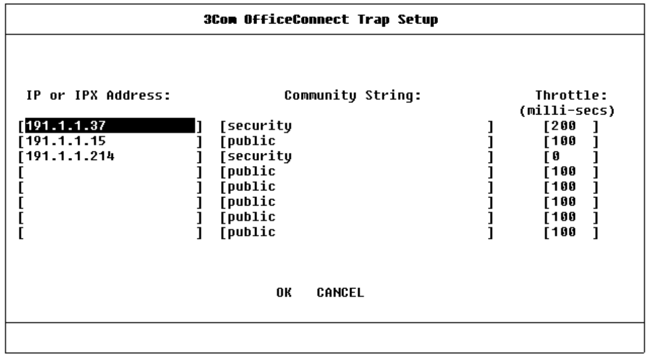
SETUP TRAPS Press [Return] when the *SETUP TRAPS* button is highlighted to set up the parameters for traps.

CONSOLE PORT Press [Return] when the *CONSOLE PORT* button is highlighted to set up the console port parameters.

CANCEL Press [Return] when the *CANCEL* button is highlighted to abandon this screen without actioning any changes, and return to the Main Menu.

Setting Up Traps

The Trap Setup screen, as shown in Figure 5-6, is used to set up *traps*. Traps are messages sent across the network to an IP/IPX-based network management application which inform the network manager of the status of your hub.



```
                        3Com OfficeConnect Trap Setup

 IP or IPX Address:            Community String:              Throttle:
                                                             (milli-secs)
[191.1.1.37         ]  [security                        ]      [200  ]
[191.1.1.15         ]  [public                          ]      [100  ]
[191.1.1.214        ]  [security                        ]      [0    ]
[                   ]  [public                          ]      [100  ]
[                   ]  [public                          ]      [100  ]
[                   ]  [public                          ]      [100  ]
[                   ]  [public                          ]      [100  ]
[                   ]  [public                          ]      [100  ]

                              OK   CANCEL
```

Figure 5-6 Trap Setup Screen

Your Transcend IP/IPX-based network manager may automatically set up the trap destination addresses for you. Check the accompanying documentation.

IP or IPX Address Enter the IP or IPX address of the remote network management station to which SNMP traps should be sent.

Community String The community string allows a very simple method of authentication between the hub and the remote network management station. You can enter any text string of up to 32 characters (case sensitive). The remote network management station must be configured to look for traps sent with this community string, otherwise it will ignore the traps. The default community string is *public*.

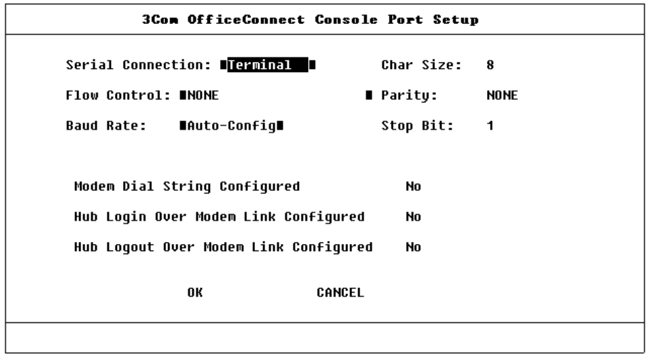
Throttle To prevent a remote network management station receiving too many traps at once, you can configure the hub to transmit traps with a delay between each trap. If several traps are generated at once, they will be transmitted with the specified delay between them. The unit of throttle is one thousandth of a second. The default value is 100, which gives a delay of one tenth of a second between each transmission. If you set the throttle to 0, traps will be sent as soon as they are generated.

If your trap configuration results in a large number of traps being generated within a short period of time, it is possible that some traps will not be sent.

Connecting a Modem to the Console Port

The Console Port Setup screen is shown in Figure 5-7. The console port is already correctly configured by default. Only alter these default settings if you are connecting a modem to the console port.

CAUTION: *Do not change any of these settings unless you fully understand what you are doing. Incorrect settings will lock you out from the hub when you select OK, and you will have to contact your supplier for information on recovering management communication.*



```
                3Com OfficeConnect Console Port Setup

   Serial Connection: Terminal           Char Size:   8
   Flow Control:  NONE                   Parity:      NONE
   Baud Rate:     Auto-Config            Stop Bit:    1

    Modem Dial String Configured            No
    Hub Login Over Modem Link Configured    No
    Hub Logout Over Modem Link Configured   No

                 OK              CANCEL
```

Figure 5-7 Console Port Setup Screen

If you alter the console port settings and select *OK*, you terminate any existing session using the console port. To avoid terminating the session completely, ensure that the settings are correct and that the connected equipment's settings match the new configuration.

If you change the console port parameters with Auto Config already set to Enabled, or if you change Auto Config to Enabled, you need to perform the *wake-up* procedure before communication is re-established, see "Main Banner" on page 5-6.

If you are unsure of the correct settings to use, refer to the manual for your terminal or modem. If you change the settings by accident, return them to their default settings (shown on these pages as the underlined values).

Serial Connection Terminal / Modem
Select Modem if you want to manage the hub through a modem. Otherwise, leave as Terminal. The cable you require for connecting a modem is shown in "Cabling" on page A-2.

Flow Control NONE / XON/XOFF / RTS - CTS Bidirectional / RTS - CTS Unidirectional
Select the flow control option that corresponds with your terminal or modem.

Speed Auto-Config / 1200 / 2400 / 4800 / 9600 / 19200
Select the baud rate for your terminal or modem. The hub can automatically configure the terminal speed to work with your VT100 terminal. Note that the setting made by automatic configuration is not displayed on the screen. Leave this field as Auto-Config if you require automatic configuration. To start automatic configuration, the wake-up procedure must be performed at your VT100 terminal.

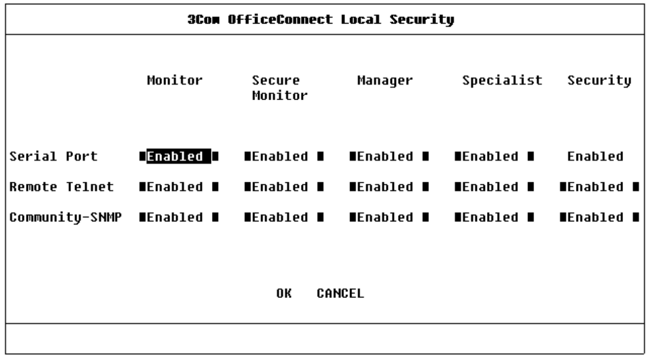
Char Size, **Parity** and **Stop Bit** are all fixed.

Modem Dial String Configured, **Hub Login Over Modem Link Configured** and **Hub Logout Over Modem Link Configured** are fields reserved for use by suppliers setting up the special modem dial-out feature, see "Remote Management Service" on page 3-7.

Configuring Local Security

The Local Security screen, as shown in Figure 5-8, is used for preventing various types of management connection. This option is available only for users with *security* access level.

The Local Security screen shows a table displaying every combination of access method (console port, Telnet or SNMP) and access level. For example, the top left field shows whether console port access by users with *monitor* access level is enabled or disabled.



3Com OfficeConnect Local Security

	Monitor	Secure Monitor	Manager	Specialist	Security
Serial Port	■Enabled ■	■Enabled ■	■Enabled ■	■Enabled ■	Enabled
Remote Telnet	■Enabled ■	■Enabled ■	■Enabled ■	■Enabled ■	■Enabled ■
Community-SNMP	■Enabled ■	■Enabled ■	■Enabled ■	■Enabled ■	■Enabled ■

Figure 5-8 Local Security Screen

The access levels are defined as:

- *Monitor* — This allows the user to view the essential operations of the hub and to establish whether or not the hub is operating correctly. A user at this level cannot change the operating parameters of the hub.
- *Secure Monitor* — In this implementation, Secure Monitor has the same rights as Monitor.
- *Manager* — This allows the user to monitor and change the operational parameters of the hub. The user cannot create or delete other users, re-initialize the hub or download a software image.
- *Specialist* — In this implementation, Specialist has the same rights as Manager.
- *Security* — This allows the user to access all the management operations. This level of security should be assigned only to the system administrator or somebody with the system administrator's responsibilities.

To prevent you from locking yourself out from the hub completely, console port access is always kept enabled for the *security* access level.

Console Port Enabled / Disabled
To prevent access to the management facilities through the console port, disable access to the facility for each access level. To allow you to configure the hub locally in the event of problems on your network, we suggest that you change the default password for the permanently-enabled security access level, see "Editing Users" on page 5-18.

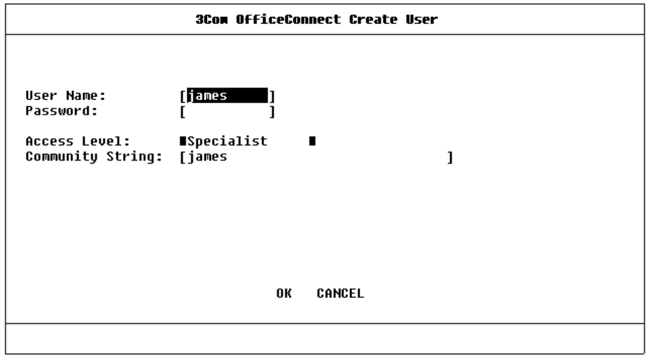
Remote Telnet Enabled / Disabled
Telnet is an insecure protocol. You may wish to disable all access to the management facilities through Telnet if there is important or secret data on your network.

Community SNMP Enabled / Disabled
The hub can be managed through SNMP using a remote network manager. Community SNMP does have some simple security features but it is an insecure protocol. You may wish to disable all access to the management facilities through Community SNMP if there is important or secret data on your network.

Configuring Users

Creating Users

The Create User screen, as shown in Figure 5-9, is used to add new users. This option is available only for users with *security* access level. There can be up to 10 users, including the three default users. Up to three users can concurrently access the management facility using Telnet. There is no limit to the number of SNMP remote management sessions.



```
                 3Com OfficeConnect Create User

User Name:        [james     ]
Password:         [          ]

Access Level:     ▮Specialist     ▮
Community String: [james                          ]

                         OK   CANCEL
```

Figure 5-9 Create User Screen

User Name Enter the name of the user. The name can be up to 10 characters. The user name is case sensitive.

Password Enter a password for this user. The password can be up to 10 characters. The password is case sensitive and is not displayed on the screen.

Access Level <u>Monitor</u> / Secure Monitor / Manager / Specialist / Security
Enter an appropriate access level for the new user by cycling through the options using the space bar.

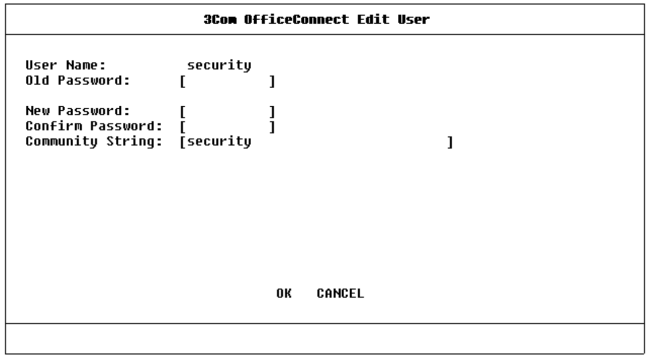
Community String By default, the community string is the same as the User Name. You can change this string to any text string of up to 32 characters. The community string is used only for SNMP access. The remote network manager must be configured to use the same community string.

Each user's community string must be unique.

Editing Users

The Edit User screen, as shown in Figure 5-10, is used to change your own password or community string. This option is available only for users with *security* access level.

No user can directly change another user's password or community string. If you are a system administrator and wish to change another user's password, you need to log on as the other user.



```
                    3Com OfficeConnect Edit User

User Name:          security
Old Password:      [          ]

New Password:      [          ]
Confirm Password:  [          ]
Community String:  [security                     ]
```

Figure 5-10 Edit User Screen

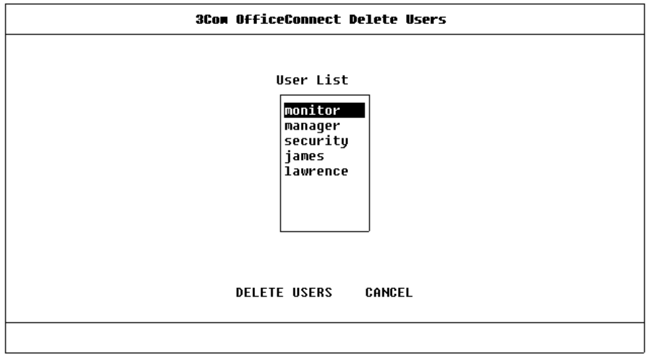
The options are similar to the Create User screen, see "Creating Users" on page 5-17. The main differences are the password fields. You must type in your current password in the *Old Password* field before you can change any fields. To set a new password, enter the password in both the *New Password* and *Confirm Password* fields.

If you enter different values for the *New Password* and *Confirm Password* fields, an error message is displayed when the *OK* button is selected. If [Return] is then pressed, a null password is set for the user. The user can log in but if an attempt is made to change the password again, the message 'Old Password Field Not Completed' is displayed.

If you forget your password, refer to the advice in "Problems When Using Quick Config Manager" on page 6-3.

Deleting Users

The Delete Users screen, as shown in Figure 5-11, is used to remove users from the User List. The User List shows all of the users configured for the hub. This option is available only for users with *security* access level.



3Com OfficeConnect Delete Users

User List

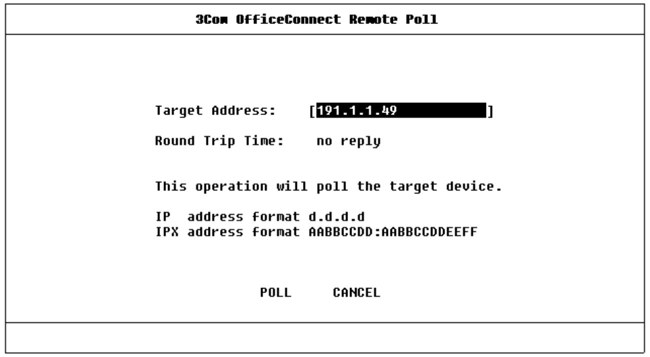
```
monitor
manager
security
james
lawrence
```

Figure 5-11 Delete Users Screen

Select the users to delete from the List Box using the spacebar, then move to the *DELETE USERS* button and press [Return]. You cannot delete the current user (the user name you used to log on) or any of the default users (monitor, manager or security).

Polling a Remote Device

The Remote Poll screen, as shown in Figure 5-12, is used to see if a remote device is responding, by sending a message forcing a response from the target device. This determines if there is a path or a congested path between this device and other devices on the network. This option is available only for users with *manager* access level or higher.



3Com OfficeConnect Remote Poll

```
Target Address:    [191.1.1.49          ]

Round Trip Time:    no reply

This operation will poll the target device.

IP  address format d.d.d.d
IPX address format AABBCCDD:AABBCCDDEEFF
```

Figure 5-12 Remote Poll Screen

The OfficeConnect Hub 8/TPM must have an IP or IPX address configured for it, to enable it to receive responses from the device it is polling.

Target Address Enter the IP or IPX address of the device to poll.

If there are multiple instances of the Remote Poll screen, they share the same Target Address. This may happen if there are multiple Telnet sessions, or a console port session and a Telnet session. The last address entered is the address that is polled.

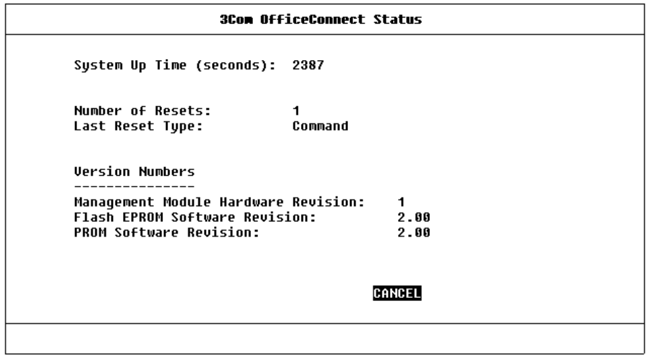
Round Trip Time This is the interval in milliseconds between the time the last frame was sent to the target device and the time a response was received by the hub. If there is no response within a few seconds, no reply is shown. Also displayed is the number of router hops and, if set, the time-to-live for the frame.

The hub can be configured to automatically poll several devices at regular intervals, and report back to an IP/IPX-based network management application if there is no response.

Viewing Internal Version Numbers

The Status screen, as shown in Figure 5-13, shows information about the hub.

Make a note of this information as your supplier may need to know it should you contact them with a problem.



```
                       3Com OfficeConnect Status

        System Up Time (seconds):  2387


        Number of Resets:          1
        Last Reset Type:           Command


        Version Numbers
        ---------------
        Management Module Hardware Revision:    1
        Flash EPROM Software Revision:          2.00
        PROM Software Revision:                 2.00


                                                   CANCEL
```

Figure 5-13 Status Screen

System Up Time This field indicates how long the hub has been running since the last reset.

Number of Resets This field shows the total number of resets since the hub was first installed, or initialized.

Last Reset Type This field indicates the cause of the last reset.

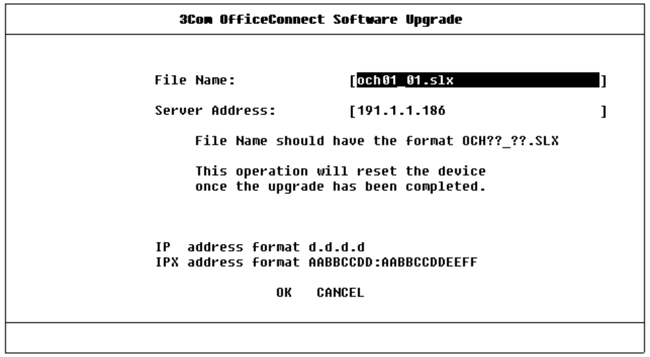
Management Module Hardware Revision This is the hardware version of the management board inside the hub.

Flash EPROM Software Revision This is the version number of the software image stored in the management board's memory.

PROM Software Revision This is the version number of software stored in the Boot PROMs on the management board.

Downloading a Software Upgrade

The Software Upgrade screen, as shown in Figure 5-14, is used to download a new version of the software image to the hub. This option is available only for users with *security* access level.



```
                 3Com OfficeConnect Software Upgrade

          File Name:              [och01_01.slx                 ]
          Server Address:         [191.1.1.186                  ]
               File Name should have the format OCH??_??.SLX

               This operation will reset the device
               once the upgrade has been completed.


          IP  address format d.d.d.d
          IPX address format AABBCCDD:AABBCCDDEEFF

                         OK   CANCEL
```

Figure 5-14 Software Upgrade Screen

When 3Com issues a new version of the hub SmartAgent® software, you can obtain the software image from 3Com bulletin board services, see "3Com provides easy access to technical support information through a variety of services. This appendix describes these services." on page C-1.

The software download can be performed through a serial connection (over SLIP) but it is much faster over the network.

File Name Enter the name of the file that contains the software image to be downloaded to the hub. You must place the image file where it is accessible to the TFTP load request. Check with your supplier if you are unsure where to place the image file.

You may wish to download the file from another directory. If so, you must give the full path to the file and the filename, using a maximum of 30 characters.

Server Address Enter the IP or IPX address of the device where the software file containing the image of the management facility can be found.

OK Select this button to start the software download. When the download is complete, the hub is reset.

If the software download fails, any traps that are sent to an IP/IPX-based network manager, reporting the failure, may indicate an incorrect status. This is not a concern for a successful download as it always result in a correct trap status.

6 PROBLEM SOLVING

The OfficeConnect® Hub 8/TPM has been designed to aid you when detecting and solving possible problems with your network. These problems are rarely serious, the cause is usually a disconnected or damaged cable, or incorrect configuration. If this chapter does not solve your problem, contact your supplier for information on what to do next.

Perform these actions first:

- Ensure all equipment is powered on.
- Power each hub off, wait about 5 seconds and then power them on so they perform a self-test. The self-test only takes a few seconds, during which all LEDs light. Port Status LEDs light yellow.

Isolating a Problem

A good way of isolating a problem is to see whether it occurs on a particular port only. This can be done by:

- Using a different port to see if the problem still exists.
- Using management to view how a port has been set up. In particular, see if the port is:
  - Partitioned because of a network loop
  - Disabled by management
  - Part of a resilient link pair
  - Performing security

Check the Alert LED and if lit, use the Alerts dialog box in Quick Config Manager to see what condition is causing it to light.

Problems When Using Your Hub

Power LED not lit. Check your power adapter connection. If there is still no power, you may have a faulty power adapter which needs replacing with another OfficeConnect power adapter. **Do not use any other power adapter with the hub.**

Alert LED continuously lit. If you haven't configured the Alert LED, it lights for two default conditions. It could be that there is either continual excessive use of your network (over 80%) or, more likely, a 10BASE-T port has partitioned due to a loop in your network (in which case a Port Status LED is yellow). Examine your connections and remove the loop. Each piece of equipment needs only one connection to your OfficeConnect hub.

If you have configured the Alert LED, check the Alerts dialog box in Quick Config Manager to see what conditions have caused the LED to light, see "Setting Up the Alert LED" on page 4-15.

Check that the Alert LED Test is disabled, in the Alerts dialog box. If it is not, select Disable and click on OK.

Port Status LED yellow for a 10BASE-T port. It is likely that there is a loop in your network which has caused this port to partition. Examine your connections and remove the loop. Each piece of equipment needs only one connection to your OfficeConnect hub.

Port Status LED not lit for a 10BASE-T port that has a connection. There is a problem with this connection. Check you are using a 'Straight-through' 10BASE-T cable which is properly connected at both ends, is not damaged, and that the equipment it is connected to is powered on and operating correctly.

Link between two OfficeConnect hubs not working. Check your hub connections; follow the information given in "Connecting OfficeConnect Hubs Together" on page 2-8. With 10BASE-T it is likely an MDI/MDIX switch is set incorrectly. With 10BASE-2 (Coax) it is likely a terminator (end piece) is not fitted properly; this would cause the Coax Port Status LED to light yellow (partition).

Problems When Using Quick Config Manager

You cannot access the hub. For a successful local management connection, you need to use a standard null modem cable, and have the hub's console port set to 9600 baud (or autoconfiguration enabled), the serial connection type set to 'Terminal', and the flow control set to 'NONE'. These are the default settings. For information on the console port settings, see "Connecting a Modem to the Console Port" on page 5-13.

You forget your community string. Log in to the hub using VT100, and use the Edit User screen to view your community string, see "Editing Users" on page 5-18.

Problems When Using VT100

The initial VT100 Main Banner screen does not display. Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

For console port access, check you have performed the wake-up procedure correctly, by pressing [Return][Return].

Check the settings on your terminal or emulator. The parity must be set to 'none', the stop bit '1' and the character size '8'. The management facility's autoconfiguration works only with speeds from 1200 to 19200 baud.

Check that autoconfiguration is not disabled.

If you still cannot access the hub, reset the hub using Quick Config Manager, see "Resetting the Hub" on page 4-11, and retry the wake-up procedure. If this does not work, initialize the hub.

Screens are incorrectly displayed. Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

Check the settings on your terminal or emulator. The parity must be set to 'none', the stop bit '1' and the character size '8'. The management facility's autoconfiguration works only with speeds from 1200 to 19200 baud.

The Telnet management station cannot access the device. Check the hub's IP address, subnet mask and default router are correctly configured, see "Giving the Hub an IP Address" on page 4-7, and the device has been reset. Ensure that you enter the IP address correctly when invoking the Telnet facility.

You forget your password.
Another user with *security* access level can log in using VT100, delete your user name, and create a new user name, with a new password for you, see "Configuring Users" on page 5-17.

If you know your community string, you can log in using Quick Config Manager and initialize the device, see "Initializing the Hub" on page 4-11. This returns all configuration information, including passwords, to the default values.

Alternatively, another user with *security* access level can log in and initialize the device.

Problems When Using an IP/IPX-based Management Application

The IP/IPX-based management application cannot access the device. Check that:

- The hub's IP address, subnet mask and default router are correctly configured, see "Giving the Hub an IP Address" on page 4-7.
- The hub has been reset, see "Resetting the Hub" on page 4-11.
- The hub's IP address is correctly recorded by the IP/IPX-based management application. For information on how to do this, refer to the documentation accompanying the application.

Traps are not received by the IP/IPX-based management application. Check that the address of the management station is entered in the hub's trap table, see "Setting Up Traps" on page 5-12.

The IP/IPX-based management application can no longer access the device. Check that Community-SNMP access is enabled, see "Configuring Local Security" on page 5-15.

Check that the port through which you are trying to access the hub has not been disabled. If it is enabled, check the connections and network cabling at the port. Try accessing the hub through a different port. If you can now access the hub, a problem with the original port is indicated. Re-examine the connections and cabling.

Possibly there is a network problem preventing you from accessing the hub over the network. Try accessing the hub through the console port, and reset the hub.

A DIMENSIONS, STANDARDS AND CABLING

Dimensions and Operating Environment

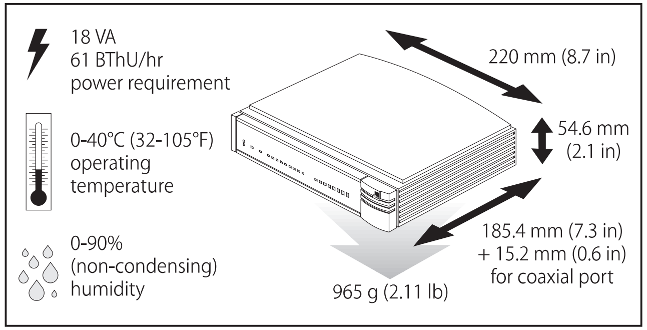


Figure A-1 Dimensions And Operating Environment For The Hub

BABT Approval (for U.K. Users Only)

The OfficeConnect® Hub 8/TPM is covered by Oftel General Approval, NS/G/12345/J/100003, for indirect connection to a public telecommunications system. This can be achieved using the console port and an approved modem.

Standards

Functional:	ISO 8802/3 IEEE 802.3
Safety:	UL 1950, EN 60950 CSA 22.2 #950
EMC:	EN 55022 Class B EN 50082-1 FCC Part 15 Class B certified* CSA C108.8 Class B VCCI Class 2

[screened (shielded) cables must be used to ensure compliance with these EMC standards]

Environmental:	EN 60068 (IEC 68)

*Refer to “EMC Statements” at the back of this user guide for conditions of operation.

Cabling

10BASE-T

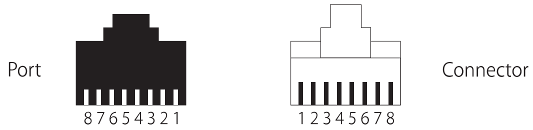


Figure A-2 Pin Numbering For 10BASE-T

Straight-through

TxD+	1	1	TxD+
TxD-	2	2	TxD-
RxD+	3	3	RxD+
RxD-	6	6	RxD-

Pins 4, 5, 7 and 8 are not used

Figure A-3 Straight-through 10BASE-T Cabling

Crossover

TxD+	1	3	RxD+
TxD-	2	6	RxD-
RxD+	3	1	TxD+
RxD-	6	2	TxD-

Pins 4, 5, 7 and 8 are not used

Figure A-4 Crossover 10BASE-T Cabling

Console Port

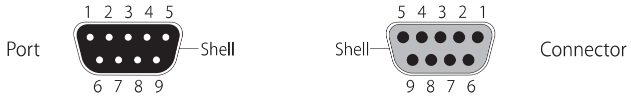


Figure A-5 Pin Numbering For Serial Connection

Examples of Null Modem Cables You Can Use

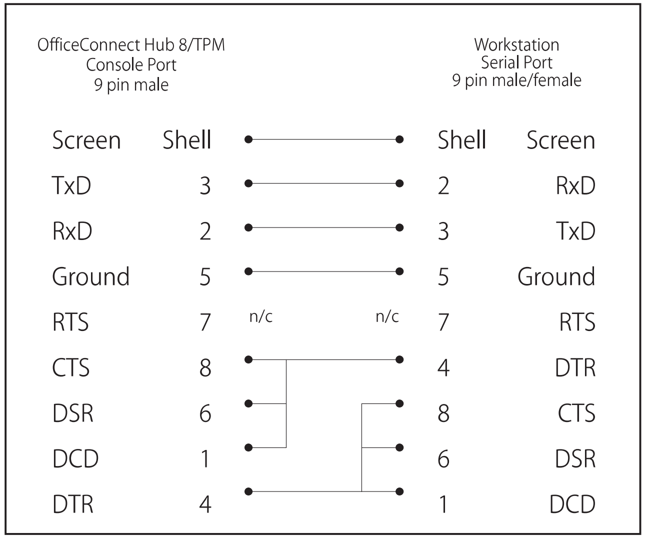


Figure A-6 Example Of Null Modem Cabling For 9 Pin Workstation

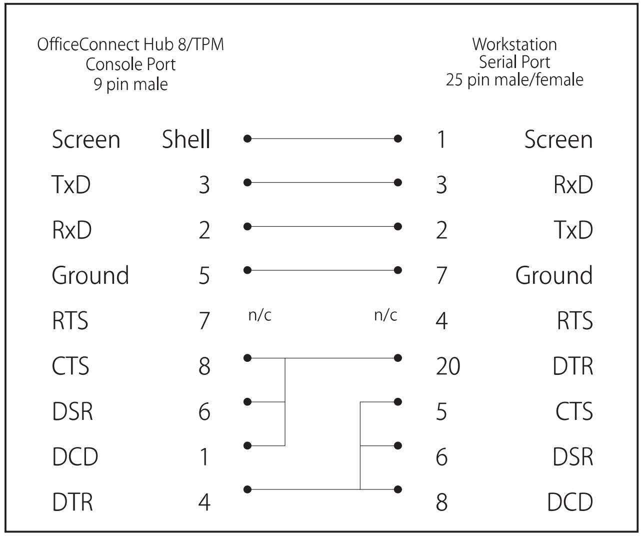
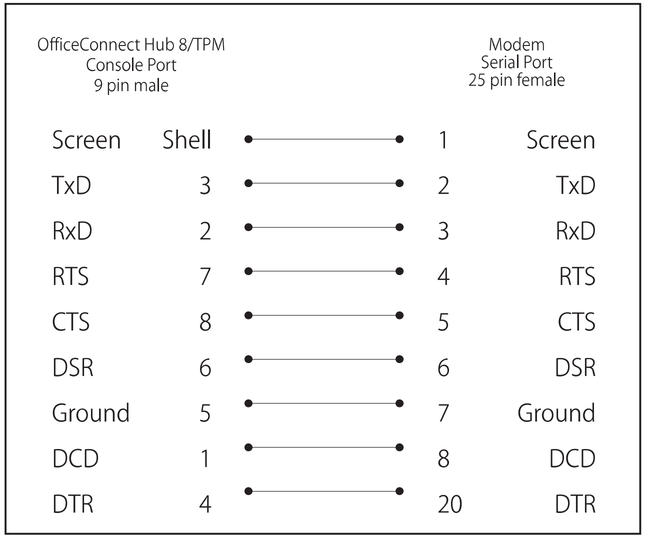


Figure A-7 Example Of Null Modem Cabling For 25 Pin Workstation

Modem Cable



OfficeConnect Hub 8/TPM Console Port 9 pin male		Modem Serial Port 25 pin female	
Screen	Shell	1	Screen
TxD	3	2	TxD
RxD	2	3	RxD
RTS	7	4	RTS
CTS	8	5	CTS
DSR	6	6	DSR
Ground	5	7	Ground
DCD	1	8	DCD
DTR	4	20	DTR

Figure A-8 Modem Cabling For 25 Pin Modem

Management Settings

You need to set your management equipment to:

- *Character size* — 8
- *Stop bit* — 1
- *Parity* — None

B IP AND IPX ADDRESSES

IP Addresses

A world-wide network such as the Internet needs a globally-accepted method of identifying individual devices (workstations and network equipment). Devices on the Internet are assigned unique addresses. The Internet then behaves like a virtual network, using these assigned addresses when sending or receiving packets.

Internet addressing uses a 32-bit (or 4 octet) address field. The bits that make up an Internet address are divided into two parts:

- The first part identifies the network on which the device resides.
- The second part identifies the device itself.

Devices attached to the same network must have the same number assigned to the network portion of the address, but have different numbers assigned to the device portion of the address.

To ensure the uniqueness of Internet addresses, they are assigned by three organizations, NIC, RIPE and APNIC-DOM. These organizations assign a globally unique network number to each network that wants to connect to the Internet. They only assign the network portion of the address; assigning the device numbers is your responsibility.

If you do not plan to connect to the Internet but need to use IP addresses on your network, you could assign network numbers on your own. However, NIC, RIPE and APNIC-DOM still assign and register unique network numbers to organizations not planning to join the Internet. This means that if you change your mind later, you can simply connect to the Internet without having to obtain new network numbers and reconfigure every device on your network with a new address.

For information on assigning your own IP addresses for a small, contained network, see "Assigning IP Addresses to a Small, Contained Network" on page B-5.

Obtaining a Network Number

There are three organizations responsible for allocating network numbers. These details are correct at the time of printing, but may change.

USA - InterNIC, Network Solutions

Attention:	InterNIC Registration Services 505 Huntmar Park Drive Herndon VA 22070
Telephone:	1-800-444-4345 (Toll Free) 1-619-455-4600 1-703-742-4777

You can also send e-mail to these addresses:

- hostmaster@rs.internic.net
  (host, domain, network changes and updates)
- action@rs.internic.net
  (computer operations)
- mailserv@rs.internic.net
  (automatic mail service)
- info@internic.net
  (automatic mail service for general enquiries)
- refdesk@is.internic.net
  (enquiries not handled by the services above)

Europe - RIPE

Attention:	RIPE NCC Kruislaan 409 NL-1098 SJ Amsterdam The Netherlands
Telephone:	+31 20 592 5065
Fax:	+31 20 592 5090
e-mail:	ncc@ripe.net

Asia Pacific Network Information Centre (APNIC-DOM)

Attention:	Asia Pacific Network Information Centre (APNIC-DOM) c/o Computer Centre University of Tokyo 2-11-16 Yayoi Bunkyo-ku, Tokyo 113 Japan
Admin. Contact:	Nakayama, Masaya (MN89)
Telephone:	+81 3 3812 2111 ext2720
e-mail:	nakayama@nic.ad.jp
Technical Contact:	Conrad, David (DC396)
Telephone:	+81 3 3580 3781 or +81 3 3580 3784
Fax:	+81 3 3580 3782
e-mail:	davidc@apnic.net

How IP Addresses Work

To make internet addressing easier to understand, IP addresses are written in dotted decimal notation, for example:

191.0.0.72
(10111111.00000000.00000000.01001000 in binary)

The IP address field is affected by:

- Classes
- Subnets

Classes

Depending on the Class (or type) of the IP address, there are many ways that the address field can be divided into a network number and a device number. The number used to convey how an IP address is divided is determined by the most significant bits in the 32-bit address field.

There are four classes of IP addresses. Each address class begins with a unique bit pattern, which is used by the Internet software residing on your devices to identify the address class.

Class A. The highest order bit is set to 0, giving a seven-bit network number and a 24-bit device address. You can have 125 networks with 16,777,214 devices per network, and the addresses are in the range 001.xxx.xxx.xxx to 126.xxx.xxx.xxx (where xxx represents the device portion).

Class B. The two highest order bits are set to 10, giving a 14-bit network number and a 16-bit device address. You can have 16382 networks with 65,534 devices per network, and the addresses are in the range 128.001.xxx.xxx to 191.254.xxx.xxx (where xxx represents the device portion).

Class C. The three highest order bits are set to 110, giving a 21-bit network number and a 8-bit device address. You can have 2,097,152 networks with 254 devices per network, and the addresses are in the range 192.000.001.xxx to 223.255.254.xxx (where xxx represents the device portion).

Class D. This is used as a multicast address. The four highest order bits are set to 1110. Multicasting is used to send an IP datagram to all members of a *host group*. A host group is composed of a set of devices identified by a single IP address. The addresses are in the range 224.000.000.000 to 239.255.255.255.

Subnets

You can further divide your IP network into sub networks. Support for sub networks is important because the number of bits assigned to the device portion of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices.

If you have a small network (less than 254 devices) then you may decide not to have sub networks.

A *subnet mask* is used to divide the device portion of the IP address into two parts:

- The first part identifies subnet number.
- The second part identifies the device on that subnet.

The bits of the subnet mask are set to 1 if the device should treat the corresponding bit in the IP address as part of the original network number or as part of the subnet number. These bits in the mask are set to 0 if the device should treat the bit as part of the device number, as shown in Figure B-1.

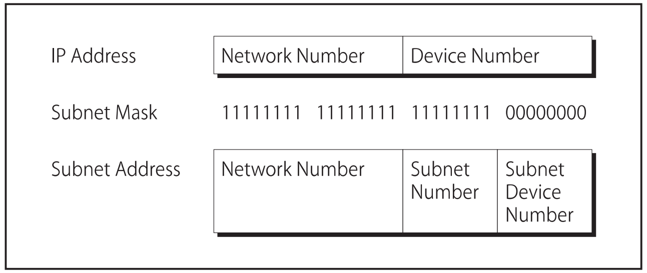


Figure B-1 Using A Subnet Mask To Obtain The Subnet Address

CAUTION: *To ensure that Quick Config Manager can always communicate with the hub, the IP subnet 192.168.101.x is permanently assigned to the SLIP port in addition to the user configurable SLIP address. Do not use this subnet for your Ethernet (network).*

Assigning IP Addresses to a Small, Contained Network

If you have a small network (less than 255 devices) that you do not plan to connect to the Internet then here is a guide as to what you can use for the IP addresses and subnet mask:

- Use an IP address that is in the range 192.000.001.xxx to 223.255.254.xxx (Class C) to define your network, and allocate device numbers (the xxx part of the IP address), starting from 1.
- Use a dummy subnet mask of 255.255.255.0 to match the network portion of your IP addresses.

Remember that no two devices on a network may have the same IP address.

IPX Addresses

If you are using the IPX protocol, the OfficeConnect® Hub 8/TPM is allocated an IPX address automatically by the local IPX router or NetWare File Server. This happens approximately 60 seconds after the hub is powered up for the first time. You should never need to change the allocated address.

C TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, we recommend that you access 3Com Corporation's World Wide Web site as described below.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Bulletin Board Service (3ComBBS)
- 3ComFacts^{SM} automated fax service
- 3ComForum on CompuServe® online service

World Wide Web Site

Access the latest networking information on 3Com Corporation's World Wide Web site by entering our URL into your Internet browser:

`http://www.3Com.com/`

This service features the latest information about 3Com solutions and technologies, customer service and support, news about the company, *NetAge*® Magazine, and more.

3Com Bulletin Board Service

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	61 2 9955 2073
Brazil	up to 14400 bps	55 11 547 9666
France	up to 14400 bps	33 1 6986 6954
Germany	up to 28800 bps	4989 62732 188
Hong Kong	up to 14400 bps	852 2537 5608
Italy (fee required)	up to 14400 bps	39 2 27300680
Japan	up to 14400 bps	81 3 3345 7266
Mexico	up to 28800 bps	52 5 520 7853
P. R. of China	up to 14400 bps	86 10 684 92351
(continued)		
Singapore	up to 14400 bps	65 534 5693
Taiwan	up to 14400 bps	886 2 377 5840
U.K.	up to 28800 bps	44 1442 438278
U.S.A.	up to 28800 bps	1 408 980 8204

Access by Digital Modem

ISDN users can dial in to 3ComBBS using a digital modem for fast access up to 56 Kbps. To access 3ComBBS using ISDN, use the following number:

408 654 2703

3ComFacts Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone using one of these international access numbers:

Country	Telephone Number
Hong Kong	852 2537 5610
U.K.	44 1442 438279
U.S.A.	1 408 727 7021

Local access numbers are available within the following countries:

Country	Telephone Number
Australia	1800 678 515
Belgium	0800 71279
Denmark	800 17319
Finland	98 001 4444

Country	Telephone Number
France	05 90 81 58
Germany	0130 81 80 63
Hong Kong	800 933 486
Italy	1678 99085
Malaysia	1800 801 777
Netherlands	06 0228049
New Zealand	0800 446 398
Norway	800 11062
Portugal	0505 442 607
Russia (Moscow only)	956 0815
Singapore	800 6161 463
Spain	900 964 445
Sweden	020 792954
U.K.	0800 626403

3ComForum on CompuServe Online Service

3ComForum is a CompuServe-based service containing patches, software, drivers, and technical articles about all 3Com products, as well as a messaging section for peer support. To use 3ComForum, you need a CompuServe account.

To use 3ComForum:

1. Log on to CompuServe.
2. Type **`go threecom`**
3. Press [Return] to see the 3ComForum main menu.

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

Contact your local 3Com sales office to find your authorized service provider using one of these numbers:

Regional Sales Office	Telephone Number
3Com Corporation	
P.O. Box 58145	800 NET 3Com *or* 1 408 764 5000
5400 Bayfront Plaza	408 764 5001 (fax)
Santa Clara, California	
95052-8145	
U.S.A.	
3Com Asia Limited	
Australia	61 2 9937 5000 (Sydney)
	61 3 9866 8022 (Melbourne)
China	8610 68492568 (Beijing)
	86 21 63740220 Ext 6115 (Shanghai)
Hong Kong	852 2501 1111
India	91 11 644 3974
Indonesia	6221 572 2088
Japan	81 6 536 3303 (Osaka)
	81 3 3345 7251 (Tokyo)
Korea	822 2 319 4711
Malaysia	60 3 732 7910
New Zealand	64 9 366 9138
Phillippines	632 892 4476
Singapore	65 538 9368
Taiwan	886 2 377 5850
Thailand	662 231 8151 4

Regional Sales Office	Telephone Number
3Com Benelux B.V.	
Belgium	32 2 725 0202
Netherlands	31 30 6029700
3Com Canada	
Calgary	403 265 3266
Montreal	514 683 3266
Ottawa	613 566 7055
Toronto	416 498 3266
Vancouver	604 434 3266
3Com European HQ	49 89 627320
3Com France	33 1 69 86 68 00
3Com GmbH	
Austria	43 1 513 4323
Czech Republic/Slovak Republic	420 2 21845 800
Germany (Central European HQ)	49 30 34 98790 (Berlin) 49 89 627320 (Munich)
Hungary	36 1 250 83 41
Poland	48 22 6451351
Switzerland	41 31 996 14 14
3Com Ireland	353 1 820 7077

Regional Sales Office	Telephone Number
3Com Latin America	
U.S. Headquarters	408 326 2093
Northern Latin America	305 261 3266 (Miami, Florida)
Argentina	541 312 3266
Brazil	55 11 546 0869
Chile	562 633 9242
Colombia	571 629 4110
Mexico	52 5 520 7841/7847
Peru	51 1 221 5399
Venezuela	58 2 953 8122
3Com Mediterraneo	
Italy	39 2 253011 (Milan) 39 6 5279941 (Rome)
Spain	34 1 383 17 00
3Com Middle East	971 4 349049
3Com Nordic AB	
Denmark	45 39 27 85 00
Finland	358 0 435 420 67
Norway	47 22 18 40 03
Sweden	46 8 632 56 00
3Com Russia	007 095 258 09 40
3Com Southern Africa	27 11 807 4397
3Com UK Ltd.	44 131 220 8228 (Edinburgh) 44 161 873 7717 (Manchester) 44 162 889 7000 (Marlow)

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S.A. and Canada	1 800 876 3266, option 2	408 764 7120
Latin America	1 408 326 2927	408 764 7120
Europe, South Africa, and Middle East	44 1442 438125	44 1442 435822
Outside Europe, U.S.A., and Canada	1 408 326 2926	1 408 764 7120

04/22/97

INDEX

Numerics

10BASE-2 1-2, 2-5
  connecting hubs 2-9
  segment 1-3
10BASE-T 1-2, 2-4, 2-5, A-2
  connecting hubs 2-10
3Com Bulletin Board Service (3ComBBS) C-1
3Com sales offices C-4
3Com URL C-1
3ComFacts C-2
3ComForum C-3

A

about network management 3-1
access levels 5-17
  manager 5-16
  monitor 5-16
  secure monitor 5-16
  security 5-16
  specialist 5-16
access method 5-15
accessing the hub 4-6
Activity and Errors graph
  broadcast frames 4-20
  collisions 4-20
  readable frames 4-20
  runts 4-20
  total errors 4-20
additional management 4-39
Alert LED 4-15
  checking 6-1
  testing 4-16
Alerts dialog box 4-15
alignment errors 4-24
assigning IP addresses B-5
attached station 4-27
authentication failure 4-17
authorized addresses 4-29
Auto Logout screen 5-9
autoconfiguration 3-4, 5-6

B

before you start 2-4
bitmap 4-7, 4-12
BOOTP 5-11
  select 5-11
broadcast frames 4-20, 4-22
bulletin board service C-1
buttons 5-2

C

cabling A-2
char size (console port setup) 5-15
checking hub connections 2-11
choice fields 5-2
classes B-3
clipping hubs together 2-6
clips 2-6
coaxial 1-2
collision 1-3, 4-20
colors
  device monitoring 4-39
  port 4-12
  resilient link pair 4-35
COM port,changing 4-3
community SNMP access 5-16
community string
  changing 5-18
  entering 5-17
  hub 4-6
  network manager 5-13
  trap 5-13
Community/Polling dialog box 4-6
CompuServe C-3
Configure menu
  Community/Polling 4-6
  General Info 4-13, 4-15, 4-32, 4-35, 4-38
  IP Configuration 4-8
configuring
  Alert LED 4-15
  IP 4-7
  port 4-25
  resilient links 4-33
connecting

a modem to the console port 5-13
management 3-3
workstations 2-7
connecting hubs together 2-8
using 10BASE-2 (Coax) 2-9
using 10BASE-T 2-10
connections
checking 2-11
hub 2-5
workstation 2-4
console port 3-4, 5-13, A-3
autoconfiguration 5-15
changing the management station's port 4-3
enabling/disabling access 5-16
management 3-4
terminal emulator, connecting 3-5
VT100 terminal
connecting 3-5
Console Port Setup screen 5-13
contact 4-9
contract ID 4-9
control keys 5-3
conventions 2
Create User screen 5-17
creating
resilient links 4-35
crossover 4-35, A-2

D

data link protocol 5-12
default
COM port 4-3
passwords 5-8
router 5-10
users 5-8
values, note 4-1, 5-1
Delete Users screen 5-19
device 1-3
general information 4-13
IP address 5-10
name 4-9
subnet mask 5-10
diagnostic LEDs 2-1
dialog box
Alerts 4-15
Community/Polling 4-6
IP Configuration 4-8
MIB II 4-13
Port Configuration 4-26
Port Security 4-29
Resilience 4-35
Security Configuration 4-32
Workgroup 4-38
dimensions A-1
disable port 4-25
Disconnect Unknown Device 4-28
displaying graphs and charts 4-18
DUD 4-28

E

Edit User screen 5-18
emergency contact 4-9
enable port 4-25
entry fields 5-2
environment A-1
equipment, connecting 2-7
error rate 4-18
Ethernet 1-2
expanding your network C-1

F

fax service. *See* 3ComFacts
FCS errors 4-24
feet 2-6
Flash EPROM software revision 5-21
flow control 5-15
frame 1-3
Frame Types chart
broadcast frames 4-22
multicast frames 4-22
unicast frames 4-22

G

general information
device 4-13
getting started 1-1
glossary 1-2
graphical representation of the hub 4-7, 4-12

H

hardware revision 5-21
how IP addresses work B-3
how to use this guide 1
hub
clipping 2-6
connecting equipment 2-7

connecting to another hub 2-8
connections 2-5
double-clicking 4-12
general information 4-13
getting started 1-1
graphical representation 4-7, 4-12
initializing 4-11
IP address 4-7
managing 3-2
monitoring other devices 4-37
port configuration 4-25
positioning 2-5
problems 6-2
resetting 4-11
security 4-28
siting 2-5
statistics 4-19
wall mounting 2-7
hub level security 4-31
HyperTerminal 3-5

I

image file name 5-22
implementation overview 2-1
Important Safety Information 7
inactivity timer 5-9
in-band management 3-6
initializing the hub 4-11
installating Quick Config Manager 4-1
Internet protocol 1-4
IP 1-4, 3-1, 4-7
IP address 4-9, B-1
allocation of B-2
network manager 5-13
obtaining an B-2
IP Configuration dialog box 4-8
IP/IPX-based network management application 3-6
IPX 1-4, 3-1
address B-6
network 5-11
network manager address 5-13
isolate 1-2
isolating a problem 6-1

K

keys (VT100) 5-3

L

L'information de Sécurité Importante 9
LAN 1-2
last restart type 5-21
late events 4-25
learn stations 4-27
LEDs 2-1
links
main and standby 4-33
state 4-27
traps 4-27
list box 5-2
local area network 1-2
Local Security screen 5-15
login violation 4-17
logoff 5-9
logon 5-7
Logon screen 5-7
loop 1-2, 2-8

M

MAC address 4-25, 5-10
Main Banner screen 5-6
main link 4-33
Main Menu screen 5-9
management
connections 3-3
settings A-4
station 3-1
tasks 3-2
management facility (VT100)
logoff 5-9
logon 5-7
starting 5-6
manager IP address 4-10
managing
over the network 3-6
through the console port 3-4
with IP/IPX-based network management application 3-6
with Quick Config Manager 3-5
with VT100 terminal 3-5
with VT100 terminal emulator 3-5, 3-6
your hub 3-2
map
Quick Config Manager windows 4-3
VT100 screens 5-4
MDI/MDIX switch 2-10, 4-34
media type 4-27
MIB 1-3, 4-13

MIB II dialog box 4-13
modem 1-4, 5-13, A-4
modem dial-out 3-7
monitor failure 4-17
monitoring 4-18
  other devices 4-37
mounting 2-7
multicast frames 4-22

N

Need To Know 4-28
NetWare file server B-6
network 1-2
  error rate 4-18
  expanding C-1
  glossary 1-2
  loop 1-2, 2-8
  management 3-1, 3-6
  manager community string 5-13
  operating system 2-4
  terminology 1-2
  utilization 4-18
Network Errors graph
  alignment errors 4-24
  FCS errors 4-24
  late events 4-25
  rate mismatch 4-25
  short events 4-24
  too long errors 4-24
  very long events 4-25
network supplier support C-4
Network Traffic graph 4-22
node (IPX) 5-11
NTK 4-28
null modem cable A-3

O

OfficeConnect hub 1-1
online technical services C-1
operating environment A-1
operating system 2-4
out-of-band management 3-4

P

packet 1-3
parity (console port setup) 5-15
partition 1-2, 4-16
  state 4-27
  traps 4-27
passwords
  changing 5-18
  creating 5-17
  default 5-8
pinouts A-2
polling 4-6
  other devices 4-37
port 2-1
  attached station 4-27
  colors 4-12
  configuration 4-25
  configure 4-25
  learn stations 4-27
  link state 4-27
  link traps 4-27
  media type 4-27
  partition state 4-27
  partition traps 4-27
  security 4-29
  security violation 4-17
  selection 4-32
  state 4-27
Port Configuration dialog box 4-26
Port Security dialog box 4-29
positioning your equipment 2-5
power A-1
problem solving 6-1
problems
  using Quick Config Manager 6-3
  using VT100 6-3
  using your hub 6-2
product range C-1
PROM software revision 5-21

Q

Quick Config Manager 3-1, 3-3, 3-5, 4-2
  installing 4-1
  problems 6-3
  using 4-1
quick installation
  connecting equipment 2-7
  management software 4-2
QUICKMGR.INI file 4-3

R

rate 4-39
  mismatch 4-25
readable frames 4-20

remote management service 3-7
Remote Poll screen 5-19
remote telnet access 5-16
reseller support tool 3-7
resetting the hub 4-11
resilience 4-33
Resilience dialog box 4-35
resilient links 4-33, 4-34
restart count 5-21
returning products for repair C-6
RJ45 1-2
round trip 4-39
round trip time 5-20
router IP address 4-10, 5-10
rubber feet 2-6
rules, resilient links 4-34
running Quick Config Manager 4-2
runt frames 4-20

S

Safety Information 7
screen
  areas 5-1
  components 5-2
  map 5-4
screens
  Auto Logout 5-9
  Console Port Setup 5-13
  Create User 5-17
  Delete Users 5-19
  Edit User 5-18
  Local Security 5-15
  Logon 5-7
  Main Banner 5-6
  Main Menu 5-9
  Remote Poll 5-19
  Setup 5-10
  Software Upgrade 5-21
  Status 5-20
  Trap Setup 5-12
security 4-28
  hub level 4-31
  port level 4-29
  violation 4-17
Security Configuration dialog box 4-32
segment 1-3
self-test 6-1
serial connection 5-14
settings A-4
Setup screen 5-10
short events 4-24
siting your equipment 2-5
SLIP 1-4, 4-10, 5-11
  address 4-10, 5-11
  parameters 4-10, 5-11
  subnet mask 4-10, 5-11
SNMP 1-3, 4-13
  community string 5-17
  enabling/disabling access 5-16
software
  image version number 5-21
  upgrade 5-21
Software Upgrade screen 5-21
speed (console port setup) 5-15
spot checks 2-11
stacking 2-8
  clips 2-6
standards A-1
standy link 4-33
starting 4-2
  Quick Config Manager 4-2
  the VT100 management facility 5-6
statistics
  activity and errors 4-19
  frame types 4-21
  network errors 4-23
  network traffic 4-22
Status screen 5-20
stop bit (console port setup) 5-15
straight-through 2-4, A-2
subnet mask 4-10, 5-10, B-4
subnets B-4
supplier support tool 3-7
support contract 4-9
system up time 5-21

T

target address 5-20
technical support
  3Com URL C-1
  bulletin board service C-1
  fax service C-2
  network suppliers C-4
  product repair C-6
  using CompuServe C-3
technology overview 1-2
Telnet 1-4, 3-1
  accessing facility using 3-6
  control keys 5-3
  enabling/disabling access 5-16

temperature A-1
Terminal 3-5
terminal emulator 3-3, 3-5
  connecting 3-5
terminal speed 5-15
terminology 1-2
testing the Alert LED 4-16
TFTP server address 5-22
throttle 5-13
too long errors 4-24
total errors 4-20
TP 1-2
Transcend Quick Configuration Manager 3-1
trap 4-26
Trap Setup screen 5-12
traps 1-3, 4-25, 4-34, 4-37
  community string 5-13
  introduction to 5-12
  IP address 5-13
  throttle 5-13
trouble shooting 6-1
twisted pair 1-2

U
unicast frames 4-22
upgrading software 5-21
URL C-1
user guide conventions 2
user interface, overview of 5-1
user name 5-17
users
  access level 5-17
  changing community string 5-18
  changing password 5-18
  creating 5-17
  default 5-8
  deleting 5-19
  password 5-17
utilization 4-18

V
version number
  flash EPROM 5-21
  hardware 5-21
  PROM software 5-21
very long events 4-25
View menu
  Activity/Errors 4-19
  Frame Types 4-21
  Traffic 4-22
  Zoom In 4-12
VT100 1-4, 3-1
  keys 5-3
  problems 6-3
  starting 5-6
VT100 screen
  areas 5-1
  components 5-2
  map 5-4
VT100 terminal 3-3, 3-5
  emulator 3-5, 3-6
VT100 terminal, connecting 3-5

W
wake-up procedure 5-6
wall mounting 2-7
Wichtige Sicherheitshinweise 8
window map 4-3
Windows 3-1
Workgroup dialog box 4-38
workgroup monitor failure 4-17
workstation connections 2-4
World Wide Web (WWW) C-1

Z
Zoom view 4-12

LIMITED LIFETIME WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	One year
Network adapters	Lifetime
Ethernet stackable hubs and Unmanaged Ethernet fixed port repeaters	Lifetime*
(One year if not registered)	
*Power supply and fans in these stackable hubs and unmanaged repeaters	One year
Other hardware products	One year
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair under warranty or not.

SOFTWARE: 3Com warrants that the software licensed from it will perform in substantial conformance to the specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the media containing software against failure during the warranty period. 3Com’s sole obligation with respect to this express warranty shall be (at 3Com’s discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media. 3Com makes no warranty or representation that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

WARRANTIES EXCLUSIVE: IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95052-8145
(408) 764-5000
18th March 1996

EMC Statements

FCC STATEMENT: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CSA STATEMENT: This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI STATEMENT:

この装置は、第二種情報処理装置(住宅地域又はその隣接した地域において使用されるべき情報処理装置)で住宅地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(ＶＣＣＩ)基準に適合しております。

しかし、本装置をラジオ、テレビジョン受信機に近接してご使用になると、受信障害の原因となることがあります。

取扱説明書に従って正しい取り扱いをして下さい 。

The user may find the following booklet prepared by the Federal Communications Commission helpful:

'How to Identify and Resolve Radio-TV Interference Problems'

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.